TRABAJO FIN DE GRADO

Universidad Carlos III de Madrid

Escuela Politécnica Superior

Grado en Ingeniería en Tecnologías de Telecomunicación

Selección de Proveedores de Servicios Cloud basada en métricas de seguridad

Autor : Iciar González González

Tutoras: Patricia Arias Cabarcos y Florina Almenares Mendoza

Octubre 2015

Trabajo Fin de Grado

Selección de Proveedores de Servicios Cloud basada en métricas de seguridad

Autor

Iciar González González

Tutoras

Patricia Arias Cabarcos

Florina Almenares Mendoza

Realizado el acto de defensa y lectura del Trabajo Fin de Grado el día __ de Octubre de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, el tribunal:

PRESIDENTE:

SECRETARIO:

VOCAL:

acuerdan otorgarle la calificación de:

CALIFICACIÓN:

Leganés, a de Octubre de 2015

Agradecimientos

En primer lugar, me gustaría agradecer la ayuda y el interés mostrado en todo momento por mis tutoras, Patricia y Florina.

A mis padres y a mi hermana por su apoyo incondicional durante todos estos años. Gracias por vuestra confianza y ayuda, y por recordarme que todo esfuerzo tiene su recompensa.

A Sergio, por haberme acompañado a lo largo de este camino. Gracias por estar ahí y ayudarme.

También agradecer a mis compañeros de clase y amigos por apoyarme en todo momento.

Gracias

"Nunca consideres el estudio como una obligación, sino como una oportunidad para penetrar en el bello y maravilloso mundo del saber"

Albert Einstein (1879-1955)

Resumen

Uno de los servicios tecnológicos que está en pleno desarrollo y uso por parte de numerosas industrias es el Cloud. A lo largo del tiempo hemos sido testigos de los múltiples cambios que ha sufrido el sector tecnológico pero pocos avances han sido tan significativos como el desarrollo de este servicio así como la entrada de numerosos proveedores globales que lo ofrecen. Este servicio Cloud permite dar cobertura a gran cantidad de empresas permitiendo el acceso ubicuo y bajo demanda a un conjunto compartido de recursos de computación, lo cual ha supuesto una revolución de la que se benefician tanto consumidores finales como empresas públicas o privadas. La seguridad en este servicio ha sido uno de los principales problemas, pues lo datos del usuario pasan a estar almacenados en servidores ajenos, por todo esto, los aspectos de seguridad cobran una gran importancia ya que estamos subcontratando infraestructura (IaaS), plataforma (Paas) y software (SaaS) a un tercero el cual maneja nuestros datos.

Por otro lado, en la época actual, la exploración de la mayor productividad y eficiencia fomentan la búsqueda de nuevos métodos para afrontar la toma de decisiones en escenarios donde intervienen gran número de criterios o alternativas de selección. Por consiguiente, es necesario utilizar herramientas que permitan discernir entre estos proveedores Cloud para así obtener una solución que satisfaga, en la mejor medida posible, la combinación de las distintos criterios así como el proveedor que más seguridad nos otorgue siendo esta de principal importancia. Dentro de esta búsqueda de nuevas metodologías se encuentran los métodos de decisión multicriterio en los cuales se centra este Trabajo Fin de Grado.

Si unificamos el aumento de la demanda de los servicios Cloud así como del número de proveedores que ofrecen este servicio con los métodos de decisión multricriterio, obtenemos como resultado la búsqueda de la mayor eficiencia posible mediante una selección correcta de un proveedor que se adapte de la mejor forma posible a los criterios seleccionados por el cliente, dentro de estos criterios, los aspectos de seguridad cobran importancia pudiendo seleccionar el proveedor más adecuado conforme al nivel de protección que necesitamos.

Para ello en este Trabajo Fin de Grado se han propuesto dos tipos de metodologías basadas en decisión multricriterio para discernir entre los distintos proveedores de servicios Cloud, estas metodologías son: en primer lugar el Proceso de Análisis Jerárquico (AHP) y, en segundo lugar, la Teoría de Utilidad Multiatributo (MAUT).

Palabras clave: Multicriterio, Cloud, Proceso de Análisis Jerárquico, AHP, Teoría de Utilidad Multiatributo, MAUT, alternativas.

Abstract

One of the technological services that is in full development and use by many industries is Cloud Computing. Over time we have witnessed the many changes that have hit the technology sector but few advances have been as significant as the development of this service as well as the entry of numerous global providers that offer it. Cloud services allow a large number of companies to gain ubiquitous and on demand access to a shared set of computing resources, which has supposed a revolution that benefits both the end consumer and the public or private companies. The security in this service has been one of the main problems, as the user data happen to be stored in outside servers, for all this, the safety aspects are of key importance as outsourcing infrastructure (IaaS), platform (PaaS) and (SaaS) software to a third party which handles our data.

Moreover, at the present time, the exploration of greater productivity and efficiency encourage the search for new methods to cope with decision-making in settings where many selection criteria or alternatives are involved. For all these reasons, it is necessary to use tools to discern between alternatives for obtaining, to the greatest extent possible, the most satisfactory solution as well as the provider that most security grant us is of primary importance. In this search of new methodologies we find the multicriteria decision methods in which this project focuses.

If we combine the increased demand for cloud services and the number of providers that offer this service with multicriteria decision methods, we obtain as a result the search for maximum efficiency through proper selection of a provider that best suits the criteria selected by the client. Within these criteria, security aspects have a fundamental importance to select the right provider according to the level of protection that they need.

In this Final Project we study two types of methodologies based on multicriteria decision making mechanisms to discern between different cloud service providers, these methodologies are: first, Analytic Hierarchy Process (AHP) and, secondly, Multiattribute Utility Theory (MAUT).

Keywords: Multicriteria, Cloud, Analytic Hierarchy Process, AHP, Multiattribute Utility Theory, MAUT, alternatives.

Contenido

Lista de Figuras

Lista de Fórmulas

Parte I

Introduction

Capítulo 1
Introduction

1.1 Motivation

In recent years there has been strong growth in infrastructure and communication networks within the technology sector with a high level of cloud adoption. The National Observatory for Telecommunications and the Information Society (ONTSI) reports on the great impact of cloud computing in the gross domestic product, as for euro invested in this technology the impact would be 1.63 euros. At the same time it is estimated that by 2016 68% of companies will be adopting of the Cloud technology.

Moreover, after years of restraint in spending in Cloud Computing services, in 2015 the investment in cloud infrastructure will increase, according to an IDC report [IDC]. More specifically, Western Europe is expected to have the highest growth in cloud IT (Information Technology) infrastructure spending at 32%, well above Latin America (23%), Japan (22%) or the US (21%). This growth trend will continue at least for five years waiting that the compounded annual growth rate (CAGT) be 14% in this period, the total investment in IT infrastructure in cloud in 2019 be of 50,000 million euros assuming thus a 45% of total spending on IT infrastructure.

Otherwise, because of the cloud's very nature as a shared resource, identity management, privacy and access control are of particular concern. With more organizations using cloud computing and associated cloud providers for data operations, proper security in these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider so in this Final Project the different providers are going to be evaluated in term of security, for example, if the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations.

There are organizations such as Cloud Security Alliance (CSA), which promotes the use of best practices for securing cloud computing and provides security education and guidance to companies. These practices include the assessment of the risk of contracting a cloud service provider (CSP) or the analysis of the security requirements based on company needs.

CSA provides a useful tool for selecting cloud service providers called Consensus Cloud Assessment Initiative (CAI), a questionnaire that allows assessing the security management of a provider according to answers. However, this process can be tedious and complex for customers.

Thus, the idea of this project arises: to create a tool that automatically make that cloud service assessment easily for the customer. This tool would be composed of two parts:

- An engine that manages and analyses data security metrics of cloud services providers and a Web service to access that data.

- A web application that allows comparing with Multicriteria methods and graphically the security services from different CSPs using the data provided by the Web service.

The final tool is integrated by two related projects that implement each of the parts as is shown in Figure 1.

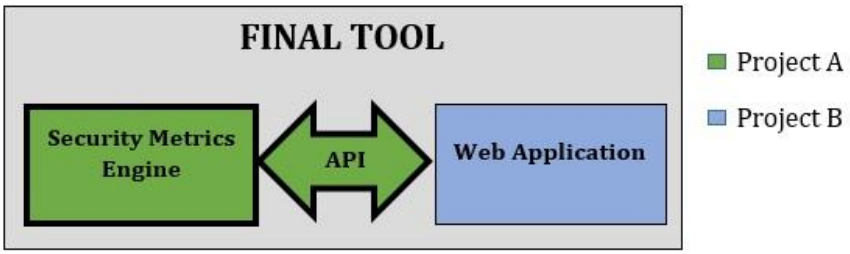


Figura 1.Tool Structure

In particular, this project corresponds to the Project B shown in Figure 1. The goal of this project is through the collection of metadata, perform the best provider selection based in security metrics with the use of multi-criteria methods.

Finally, both project come together in a joint project to integrate the final tool. This first chapter is going to describe the objectives of this Final Project and the various stages of development.

1.2 Objectives

The main objective of this Final Project is to find the provider cloud service that best works with the customer. Therefore, the analysis of the different providers is going to be through security criteria, providing an answer to one of the main problems in the field of Cloud Computing as user data happen to be stored in outside servers, managed by providers in principle not present guarantees of reliability. For this purpose, we will make

use of two Multicriteria decision methods, namely such as the Hierarchical Analysis (AHP) and Multiattribute Utility Theory (MAUT).

As for the specific project objectives are:

- Study of different types of Multicriteria decision analysis mechanisms.
- Study of Analytic Hierarchy Process (AHP).
- Study of Multi-attribute Utility Theory (MAUT).
- Develop a web application that implements AHP and MAUT and offers an interface to use these mechanisms for ranking Cloud Providers according to security criteria and select the best option. Within this objective we find the following sub-objectives:
    - Integrate the web application with an external API that provides security related data of well-known Cloud Providers Obtaining automatic metadata (JSON) and processed to obtain information related to security metrics.
    - Study of different graphics libraries to include in the web application for showing the ranking results in a user-friendly manner.
    - Implementation of a set of algorithms. Different algorithms are used to weight the criteria in decision-making, for example, one of the algorithms design calibrating the security aspects offered by providers based on the level of protection provided in respect of the 9 most important security threats in Cloud Computing ("Notorious Nine [CSA]"),other algorithms that will be implemented are AHP and MAUT.
- Test the application for a set of well-known Cloud Providers with public security documentation and evaluate the obtained results.

1.3 Stages of development

The final project was divided into the following phases of development:

- Deployment and installation of Web Server (Apache / Tomcat): at this stage took place the installation of Apache Tomcat server and initial tests were conducted to verify proper operation.

- Documentation and analysis of the state of the art: in this part the different makers multicriteria were studied, as well as the tools required for deploying and programming a web server.

- Development and testing for multicriteria decision maker Analytic Hierarchy Process for different cloud service providers.

- Development and testing for MAUT multicriteria decision maker for the various cloud service providers.

- Development and testing of the Notorious Nine algorithm for different cloud service providers

- Evaluation of results: the results obtained were analyzed and graphs were drawn.

- Final documentation and write of the work performed and the document.

1.4 Document Structure

This document is divided into several parts, which in turn are divided into various chapters. The content of each part and chapter is summarized below:

- Part One: An Introduction. In this part of the objectives, the phases of the work and structure of the document are explained. It contains a chapter:

    - Chapter 1. Introduction.

- Part Two: State of the art. Firstly the different Multicriteria methods that are used in this project are explained in detail. More specifically, Chapter 2 outlines the problem of making decisions under multiple criteria: Chapter 3 is devoted to the step-by-step description of the AHP method; Chapter 4 explains how MAUT works; Chapter 5 compares both; Chapter 6 in this chapter the nine most important security threats in Cloud Computing ("Notorious Nine [CSA]") used for processing of the algorithm are explained, this information is required to be taken as a basis for the development. Finally, the technologies used in the project are explained in Chapter 7.

- Part three: Regulatory Framework. In this section, the rule of the software used in the final project is explained. This part only contains one chapter:

    - Chapter 8. Legislation and regulatory framework.

- Part Four: Work Performed. In this part, the work necessary to develop the application it is explained. In Chapter 9, we performs the full web design application, the architectural design will be described along with its components and their functions, in Chapter 10 we will Explain in detail everything about the system implementation, and finally, in Chapter number 11 we will explain the different results obtained in the application of multi-criteria decision methods.

- Part Five: Conclusion. In this part of the documents conclusions and future work are discussed.
    - Chapter 12.Conclusions and Future Work.

- Part Six: Planning and budgeting. In this part a detailed explanation of both will be made.
    - Chapter 13. Planning.
    - Chapter 14.Budgeting.

- Part Seven: Annexes. In this part of the project information expands in some parts.
    - Annex A: Apache Tomcat settings.
    - Annex B. Criteria for the decision of the different suppliers.

Parte II

Estado Del Arte

Capítulo 2

Toma de decisiones basadas en múltiples criterios

2.1 Introducción

Toma de decisiones Multicriterios (Multiple-Criteria decision-making - MCDM) o análisis de decisión de criterios múltiples (Multiple-Criteria decision analysis - MCDA) es una subdisciplina de investigación de operaciones que considera, en la toma de decisiones, múltiples criterios.
Esta toma de decisiones [SAA94] se puede dar tanto en nuestra vida cotidiana como en entornos profesionales, una condición necesaria para que se dé un problema de decisión Multicriterio es la presencia de más de un criterio, a su vez estos criterios pueden estar en conflicto [RAM01], es decir, que el incremento de la satisfacción de uno, implique el decremento de la satisfacción del otro. Por lo que un problema puede considerarse Multicriterio si y solo si existen al menos dos alternativas de solución y al menos dos criterios que pueden estar en conflicto.
Aunque los problemas MCDM están muy extendidos en la actualidad, la vida de esta disciplina tiene una historia relativamente corta de unos 30 años, estando estrechamente relacionado con el avance de la informática.
El avance de esta disciplina en los últimos años ha hecho posible la realización de un análisis sistemático de los problemas MCDM complejos, debido al uso cada vez mayor de las tecnologías de la información y la enorme cantidad de datos que estos han generado han hecho que MDCM sea cada vez más útil e importante para el apoyo de la toma de decisiones de estos negocios. Desde el inicio de esta metodología ha habido varios avances en cuanto a la toma de decisiones con múltiples criterios, generando una gran variedad de métodos y enfoques que han ayudado al desarrollo de nuevas disciplinas.

Los Métodos de Toma de Decisiones Multicriterio han desarrollado una terminología común y propia [MAS+08] que incluye conceptos como:

- Atributos: son las características, rasgos, parámetros o cualidades que describen a cada una de las distintas alternativas. El número de atributos elegidos será decidido por el decisor o grupo de elección.

- Alternativas: son las posibles soluciones al problema de decisión que el decisor podrá elegir.

- Criterios: son los parámetros que permiten reflejar las preferencias del decisor respecto a un atributo.

- Objetivos: indican las direcciones de mejoras según lo establecido por el decisor. Es una declaración de algo que uno desea alcanzar[KEE92].

- Metas: la alternativa que recogerá los atributos ya establecidos y pueda satisfacer los criterios seleccionados acercándose lo máximo posible a los objetivos expuestos.

Actualmente, el proceso de toma de decisiones comprende las 5 primeras fases de cualquier proceso de resolución de problemas, el cual está compuesto por siete etapas [TOS+05]:

1. Una definición del problema.
2. Identificación de las alternativas.
3. Determinación de los distintos criterios.
4. Evaluación de las alternativas.
5. Elección de una opción.
6. Implementación de la decisión.
7. Evaluación de los resultados.

De estas siete etapas, las cinco primeras componen el proceso de toma de decisiones que a su vez se agrupan en dos subprocesos que son la Estructuración y el Análisis del Problema.

En la fase de Estructuración representado en la figura 2 [VAL12], se indican las posibles alternativas y se definen los criterios que se van a tener en cuenta para tomar la decisión final, en el caso de este Trabajo Fin de Grado las alternativas serán los distintos proveedores de servicios Cloud. Una vez concluida esta fase de Estructuración representado en la figura 3 [VAL12], se pasará a la fase de análisis y estudio donde se evalúan las distintas alternativas para posteriormente elegir la mejor opción.

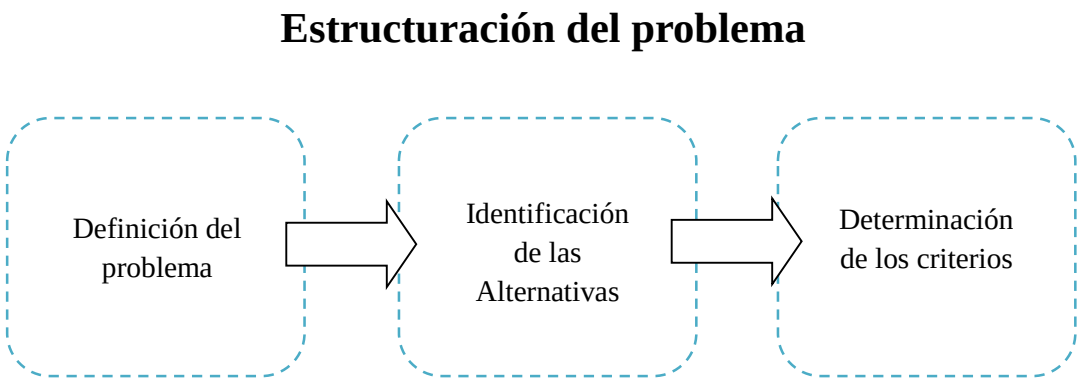


Figura 2.Estructuración del problema

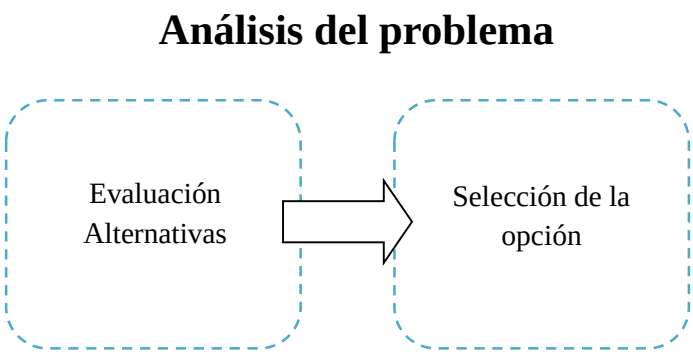


Figura 3. Análisis del problema

2.2 Tipos de MCDM/MCDA

Existen distintas clasificaciones de los problemas y métodos MCDM/MCDA. Una distinción importante entre estos problemas se basa en si las soluciones están definidas de forma implícita o explícita [HER+99].

- **Problemas de Evaluación con Múltiples criterios**: Este tipo de distinción consiste en tener un número finito de alternativas conocido explícitamente en el comienzo del proceso de solución donde cada alternativa está representada en múltiples criterios. El problema basado en este tipo de evaluación consiste en la búsqueda de la mejor o del conjunto mejor de alternativas realizada por el decisor. Las alternativas distintas también se pueden ordenar o clasificar, para realizar la ordenación habría que colocarlas en un conjunto de clases con una preferencia ordenada, mientras que para la clasificación habría que asignar las alternativas a los conjuntos ordenados.

- **Problemas de Diseño con Múltiples Criterios:** En este tipo de problemas, a diferencia con el problema expuesto anteriormente, no se conocen de forma explícita las alternativas, es decir, una alternativa se encuentra mediante la resolución de un problema matemático. El número de las alternativas puede ser finito y contable (variables discretas) o infinito y no contable (variables continuas).

2.2.1 Métodos de Decisión Multicriterio Discreta

Los métodos de Decision Multicriterio Discreta se utilizan para realizar una evaluación y decisión respecto de problemas que por diseño, admiten un número finito de alternativas de solución a través de:

- Un conjunto de alternativas estables, donde se asume que cada una de ellas es perfectamente identificada, aunque no son necesariamente conocidas en forma exacta.
- Un conjunto de criterios de evaluación que permiten evaluar cada una de las distintas alternativas conforme a los pesos que han sido asignados por el decisor y que reflejan la preferencia de cada criterio.
- Una matriz de decisión que resume la evaluación de cada alternativa en referencia a cada criterio.
- Una metodología o modelo de agregación de preferencias en una síntesis global para determina la mejor solución.
- Finalmente, un proceso de toma de decisiones.

La realización de este proyecto se centrará en los métodos de evaluación y decisión MAUT y AHP donde posteriormente se entrará en detalle con cada uno de ellos.

Capítulo 3

Proceso de Análisis Jerárquico (AHP)

3.1 Introducción

Analytic hierarchy process (AHP) es una técnica estructurada para tratar con decisiones complejas, fue desarrollada a finales de los años 60 por Thomas L.Saaty quien a partir de sus investigaciones en el campo militar junto con su experiencia formuló esta herramienta. Gracias a su simplicidad ha sido puesta en práctica en miles de aplicaciones mediante las cuales se han obtenido importantes resultados. AHP es una metodología para estructurar, medir y sintetizar así como un método matemático creado para evaluar las alternativas cuando tenemos en consideración varios criterios.

La metodología propuesta por Saaty [SAA96] debería ser simple en su construcción, adaptable a las decisiones individuales y en grupo, en consonancia con nuestros pensamientos valores e intuiciones, orientada a la búsqueda del consenso y, finalmente, una metodología que no requiera una especialización suprema para su aplicación.

3.2 Características principales

La principal característica de AHP es su modelado mediante una jerarquía [figura 4] en cuyo vértice superior se encuentra el objetivo principal o meta a alcanzar, en los niveles intermedios, se representan los criterios que seleccionados y en base a los cuales se toma la decisión, finalmente, en la base, se encuentran las distintas alternativas que se van a evaluar. Este diseño de jerarquías necesita de experiencia así como de un buen conocimiento del problema ya que precisa de toda la información necesaria.

La segunda característica que define a este método, es que cada nivel de jerarquía se basa en el uso de comparaciones entre pares de elementos, a partir de estas comparaciones se construyen matrices mediante las cuales, y haciendo uso del algebra matricial, se establecen unas prioridades con respecto a un elemento del nivel inmediatamente superior. Estas comparaciones por pares se realizan por medio de ratios de importancia o preferencia, y estos pesos o prioridades deben sumar una unidad. En resumen, el método

AHP es un modelo de decisión que interpreta datos mediante el uso de juicios y medidas en una escala de razón dentro de una estructura jerárquica.

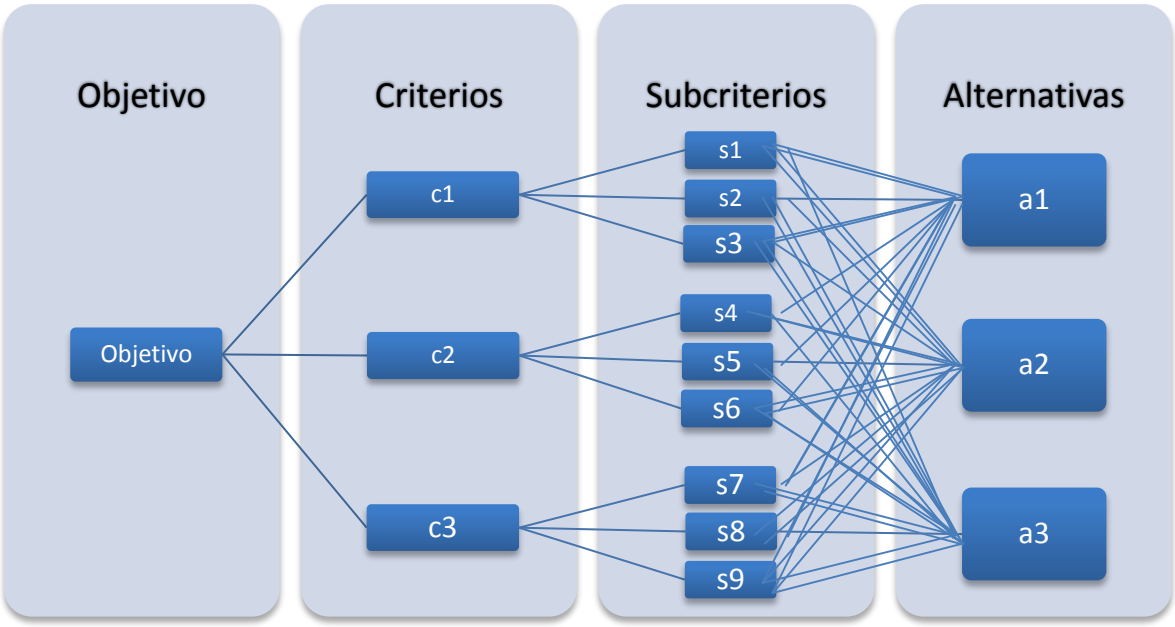


Figura 4.Modelo jerárquico para la toma de decisiones con AHP

3.3 Axiomas de AHP

Los principios en los que se basa la teoría AHP [TOS05] son:

- Independencia: Se asume que los criterios son independientes de las propiedad de las alternativas una vez se expresan preferencias.
- Homogeneidad: Las distintas preferencias se representan en una escala limitada.
- Comparación recíproca: la intensidad entre las preferencias debe ser recíproca, es decir, si Y es x veces preferido que Z, entonces Z es 1/x veces preferido que Y.
- Expectativas de orden de rango: las expectativas deben estar representadas en la estructura en términos de criterios y alternativas.

3.4 Metodología

Las etapas generales propuestas por Saaty [SAA80] en su formulación inicial son las siguientes:

- Modelización: Saaty buscó una manera de poder resolver el problema de la complejidad, para ello utilizó la estructuración jerárquica de los problemas en subproblemas homogéneos

- Valoración: en esta etapa se incorporan las preferencias y deseos de los actores mediantes los juicios incluidos en las matrices de comparación por pares, estas matrices representan la valoración relativa de un elemento frente a otro.

- Priorización y síntesis: el enfoque de AHP es totalmente sistémico ya que este método está enfocado en el sistema en general y la solución que se presenta es para la totalidad no para la particularidad.

3.5 Realización método AHP

Como primer paso, una selección adecuada de los criterios constituye una etapa fundamental en el proceso de toma de decisión, una vez se hayan definido los criterios y subcriterios formando una jerarquía descendiente [figura 4] se debe realizar la construcción de la jerarquía completa donde en el último nivel se sitúan las alternativas, el siguiente paso será construir un vector de pesos que evalúa la importancia relativa que se otorga a cada criterio. El método AHP utiliza una asignación indirecta en la cual el decisor realizada una valoración en términos cualitativos y, una vez en la escala, se obtendrán los valores numéricos que correspondan a ese valor. La escala de valores sugerida por Saaty [SAA80] es la representada en la siguiente tabla:

Valor	Definición	Comentarios
1	Igual Importancia	El criterio A es igual de importante que el criterio B
2	Importancia intermedia	Valor intermedio para cuando es necesario matizar
3	Importancia Moderada	La experiencia y el juicio favorecen ligeramente el criterio A sobre B
4	Importancia intermedia	Valor intermedio para cuando es necesario matizar
5	Importancia Grande	La experiencia y el juicio favorecen fuertemente el criterio A sobre B
6	Importancia intermedia	Valor intermedio para cuando es necesario matizar
7	Importancia Muy Grande	El criterio A es mucho más importante que el B.
8	Importancia intermedia	Valor intermedio para cuando es necesario matizar
9	Importancia extrema	La mayor importancia del criterio A sobre B esta fuera de toda duda

Figura 5.Escala fundamental de comparaciones pareadas. Fuente: [SAA80]

Una vez se cuantifican los valores, el decisor mediante la comparación entre pares debe determinar los pesos relativos de los criterios. Estos números de la escala representan la proporción en la que uno de los elementos que se consideran en la comparación por pares domina al otro respecto a una propiedad o criterio. El elemento menor tiene el valor recíproco o inverso respecto al mayor, es decir, si x es el número de veces que un elemento

domina a otro, entonces este es 1/x veces dominado por el primero de tal modo que $\frac{1}{x}$ * x = x * $\frac{1}{x}$ = 1 (principio de comparación reciproca).

Con esta jerarquía se pasa a obtener la matriz de juicios, en esta etapa el decisor debe hacer comparaciones por parejas en cada nivel de la jerarquía, la matriz que obtendremos será de tamaño n x n donde n es el número de alternativas de las que disponemos. Cada celda de la matriz de juicios contiene un valor c_{ij} este valor representa el tamaño relativo de la alternativa i respecto de la alternativa j. Los elementos de la matriz son [EDU01]:

$$c^{n\,x\,n} = \begin{cases} C_{ij} = \frac{s_i}{s_j} & \text{Proporción directa entre la entidad i respecto la j} \\ C_{ij} = 1 & \text{La entidad i y j son la misma} \\ C_{ij} = \frac{1}{s_{ji}} & \text{Inversamente proporcionales} \end{cases}$$

Fórmula 1: Matriz AHP

Si la entidad i es c_{ij} veces mayor que la entidad j, entonces la entidad j es $\frac{1}{c_{ij}}$ veces menor que la alternativa i, teniendo en cuenta esto, en la diagonal de la matriz todos los valores serán la unidad ya que se compara la misma alternativa. Para saber el valor completo de la matriz solo necesitaríamos calcular la matriz superior o inferior a la diagonal.

Habría que realizar una matriz de juicios por cada criterio a tener en cuenta en la toma de la decision final, también hay que calcular el *inconsistency index*, el cual nos proporciona la estimación de la aproximación a la consistencia perfecta.
Una matriz perfectamente consistente es aquella en la que todos sus elementos satisfacen c_{ij} x $c_{jk} = c_{ik}\ \forall\ i,j,k$. Para obtener el vector de pesos, hay que llevar a cabo el siguiente procedimiento propuesto por Saaty [SAA80]:

1. Obtener la matriz normalizada (Cnormalizada) para ello hay que dividir cada elemento de la columna j-ésima por la suma de todos los elementos de la columna.

$$C_{normalizada} = \left[C_{ijNormalizado} = \frac{c_{ij}}{\sum_{i=1}^{n} c_{ij}} \right]$$

Fórmula 2: Matriz Normalizada AHP

2. Calcular el vector de pesos (ω) promediando cada fila de la matriz normalizada, el vector ω de pesos será:

$$\hat{\omega} = \left[\hat{\omega}_1 = \frac{1}{n} * \sum_{j=1}^{n} C_{1jNormalizado} * \hat{\omega}_2 = \frac{1}{n} * \sum_{j=1}^{n} C_{2jNormalizado} \dots \hat{\omega}_n = \frac{1}{n} * \sum_{j=1}^{n} C_{njNormalizado} \right]$$

Fórmula 3: Vector de pesos AHP

3. Comprobar la consistencia de los diferentes juicios [SAA80][SAA94]:

Si C fuera una matriz consistente, λmax deberá ser igual a n. Sin embargo, el decisor cometerá un cierto grado de error en sus juicios, como resultado habrá que medir el grado de inconsistencia de los juicios emitido por el decisor. La consistencia se mide mediante el índice de consistencia o IC:

$$IC = \frac{\lambda_{maxima} - n}{n - 1}$$

Fórmula 4: Índice de consistencia AHP

4. Establecimiento de prioridades entre las alternativas:

Una vez se obtiene la ponderación de los criterios se procede a la valoración de las alternativas para calcular las prioridades locales correspondientes.
Como primer paso, para cada criterio o subcriterio se tiene que establecer una matriz de C de juicios donde se compararan dos a dos las distintas alternativas. El procedimiento que se tiene que seguir es el mismo que se ha establecido en el paso 2 pero esta vez se toma como base de comparación el grado de satisfacción de cada criterio. La escala que se usara será la misma (1/9,1/8... 1, 2…8,9).Una vez se obtenga C se procede a calcular el vector de pesos locales de las alternativas para cada criterio

5. Establecimiento de las prioridades totales asociadas a cada alternativa.

Tras obtener los vectores de prioridad para todas las alternativas respecto a un subcriterio o criterio, se obtiene una matriz la cual habrá que multiplicar por el vector de prioridad también calculado de los subcriterios respecto al criterio del cual descienden, mediante este paso se obtiene el vector de preferencias de cada alternativa respecto a un criterio.

	Criterio 1	Criterio 2	.....	Criterio 3
Alternativa 1	p_{11}	p_{12}	$\cdots$	p_{1m}
Alternativa 2	p_{21}	p_{22}	$\cdots$	p_{2m}
...	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Alternativa n	p_{n1}	p_{n2}	$\cdots$	p_{nm}

Figura 6. Matriz AHP

Se obtendrán tantos vectores de prioridad como criterios existan, con ellos se construye la matriz final que se multiplica por el vector prioridad de los criterios respecto a la meta general, dando como resultado el vector de prioridades de cada alternativa respecto del objetivo principal, permitiendo así determinar cuál alternativa es la más conveniente para la solución del problema planteado inicialmente.

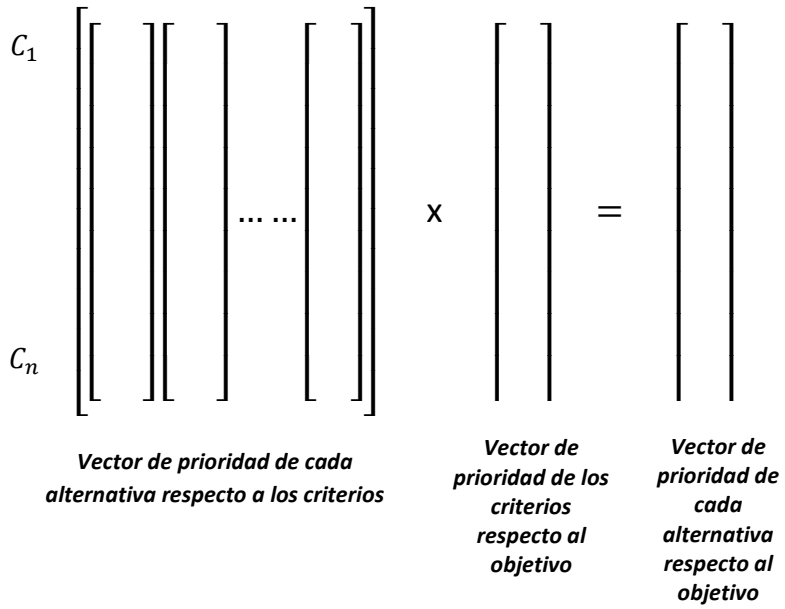


Figura 7.Generación vector de prioridad AHP

Capítulo 4

La Teoría de Utilidad Multiatributo (MAUT)

4.1 Introducción

La Teoría de Utilidad Multiatributo (Multi-Attribute Utility Theory - MAUT), es una de las metodologías más populares para la toma de decisiones Multicriterio, provee un fuerte fundamento axiomático para la toma de decisiones racional bajo múltiples objetivos[SEP03], usa funciones de utilidad para convertir las escalas de atributos numéricos a escalas de utilidad que permiten una comparación directa de diversas medidas, es decir, expresar las preferencias del decisor en términos de la utilidad que le reporta (principio de la racionalidad). La elección entre alternativas se complica por el hecho de que cada opción implica múltiples atributos que son de importancia para el decisor.
El enfoque de MAUT junto con la aparición de las funciones de utilidad y modelos de preferencia ha sido investigado y estudiado con gran detalle en un periodo de décadas por Debrey (1960), Luce y Tukey (1964), Fisgburn (1970) y Keeney y Raiffa (1976) entre otros.
Esta teoría tiene como eje principal la racionalidad y se basa en los siguientes postulados:

1. Todo decisor intenta inconscientemente maximizar una función que agrega todos los puntos de vista relevantes del problema, para ello se interroga al decisor sobre sus preferencias y sus respuestas serán coherentes con una cierta función que no será conocida a priori. El papel que desempeña el analista es de estimar la función mediante una serie de preguntas al decisor.

2. Todo par de acciones X e Y son susceptibles de ser comparadas, y existe un ordenamiento de preferencia bien definido sobre el conjunto de las acciones, de modo que para cualquier par de alternativas se tiene:

    - X>Y, es resultado X es preferido a Y.
    - X~Y, indiferencia entre X e Y.
    - X<Y, el resultado Y es preferido a X.

3. Se asume que el orden de preferencia es transitivo, es decir, si se prefiere X a Y, Y a Z, entonces se debe preferir X a Z.

Los dos últimos principios garantizan la preservación de consistencia al comparar los resultados.
Las principales fases para la aplicación correcta de MAUT son:

1. Estructurar una jerarquía de atributos: el decisor formula un conjunto de atributos para el problema.

2. Definición de las funciones de utilidad: para cada atributo se define una función de utilidad que traduce la medida del evaluador en una utilidad cuyo valor ira entre 0 y 1.

3. Transformación de las preferencias en pesos: Se utilizan pesos para caracterizar la importancia de los distintos atributos. Estos pesos se pueden obtener mediante diversos métodos.

4. Caracterización de las alternativas: para cada alternativa los atributos necesitan ser evaluados de manera cualitativa o cuantitativa.

5. Agregación de los resultados: para cada alternativa los atributos se transforman en una utilidad con las funciones del paso 2 y ponderados con los pesos del paso 3.

4.2 Objetivos

Para identificar los objetivos, los cuales deben ser medidos a través de una escala de atributos, hay que tener en cuenta una serie de consideraciones:

- Los objetivos deben estar encabezados por los objetivos fundamentales que tendrán en cuenta los aspectos del problema.
- Se consideraran como objetivos aquellos que diferencien las alternativas.
- Los objetivos no deben ser redundantes e independientes entre sí, es decir, para tratar un objetivo no se debe examinar ningún otro.
- Las escalas de medición deben medir el valor de las alternativas de manera sencilla.

4.3 Función de utilidad y modelo aditivo

MAUT tiene por objeto reducir los problemas de decisión en un contexto Multicriterio a través de una función de utilidad cardinal, la principal peculiaridad de este modelo, es la uniformidad que deben presentar las variables, es decir, antes de aplicar la ponderación para cara criterio es preciso establecer una correspondencia a cada uno de los valores con

que se miden los atributos, esto significa que deben ser transformados en utilidades. Para llevar a cabo esta transformación es necesario tomar los valores extremos máximos y mínimos de cada evaluación y hacerlos corresponder con las respectivas utilidades que irían entre 0 y 1. La utilidad 0 siempre correspondería al valor más desfavorable, mientras que el valor 1 representara el valor más favorable al evento. Para los valores intermedios habrá que realizar una proporción directa entre la utilidad mínima y máxima, la ecuación necesaria para realizar estos cálculos es la siguiente:

$$U_i(x) = 1 - \left\{ \frac{x_{min} - x}{x_{min} - x_{max}} \right\}$$

Fórmula 5: Cálculo utilidad MAUT

- El valor x_{min} es el mínimo del conjunto de observaciones.
- El valor x_{max} es el máximo del conjunto de observaciones.
- X es el valor cuya utilidad deseamos obtener.

Una vez obtenemos los valores de utilidad para los distintos atributos [ZOP+02]:

$$u(x_1, \dots, x_n) = \omega_1 * u_1(x_1) \; + \cdots + \omega_n * u_n(x_n)$$

Fórmula 6: Valores de utilidad atributos MAUT

Donde los valores $\omega_1, \dots, \omega_n$ son los pesos de cada una de las funciones de utilidad (deberán sumar la unidad).

4.4 Resolución método MAUT

Una vez tenemos calculada la matriz de utilidades para las distintas alternativas conforme los criterios, es decir, la matriz de decisión:

Criterios

Alternativas

$$\begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ u_{21} & u_{22} & \cdots & u_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n1} & u_{n2} & \cdots & u_{nm} \end{pmatrix}$$

Fórmula 7: Matriz decision MAUT

El siguiente paso es normalizar el vector de pesos de los criterios:

$$\text{Criterios} \left\{ \begin{pmatrix} \widehat{\omega}_1 \\ \widehat{\omega}_2 \\ \widehat{\omega}_3 \\ \vdots \\ \widehat{\omega}_m \end{pmatrix} \right. \quad \text{(Suma de todos los pesos =1)}$$

Fórmula 8: Vector pesos criterios MAUT

Finalmente, se multiplica la matriz de decisión con el vector de pesos de los criterios una vez normalizado, se obtiene un vector final de decisión donde cada alternativa obtiene un valor, cuanto mayor sea este valor, mayor será su utilidad.

$$\begin{pmatrix} \widehat{\omega}_1 * u_{11} + \widehat{\omega}_2 * u_{12} + \cdots + \widehat{\omega}_m * u_{1m} \\ \widehat{\omega}_1 * u_{21} + \widehat{\omega}_2 * u_{22} + \cdots + \widehat{\omega}_m * u_{2m} \\ \widehat{\omega}_1 * u_{31} + \widehat{\omega}_2 * u_{32} + \cdots + \widehat{\omega}_m * u_{3m} \\ \vdots \\ \widehat{\omega}_1 * u_{n1} + \widehat{\omega}_2 * u_{n2} + \cdots + \widehat{\omega}_m * u_{nm} \end{pmatrix}$$

Fórmula 9: Vector final MAUT

Capítulo 5
Comparativa MAUT - AHP

5.1 Introducción

AHP se diferencia de MAUT en la forma de obtener los juicios del decisor y en los principios básicos para establecer las preferencias de este.
El objetivo de MAUT es encontrar una expresión simple para los beneficios netos de una decision a través de las funciones de utilidad. Se basa en el supuesto de que el decisor sea racional, teniendo un conocimiento perfecto y coherente en sus juicios, el objetivo de este decisor será el de maximizar el valor de utilidad ya que para valores bajos en algunos criterios se pueden compensar por puntuaciones altas en otros. Por todo esto, MAUT es un tipo de MCDA conocido como “métodos compensatorios”.
En el caso de AHP, agrega diversas facetas al problema de decisión con una sola función de optimización, tiene como objetivo seleccionar la alternativa que tenga un peso mayor y es un tipo de MCDA conocido como “optimización compensatoria”. AHP se basa en el uso de métodos de comparación por pares de criterios de decision en lugar de utilidad y funciones de ponderación, todos los criterios tienen que estar emparejados con los demás y los resultados expuestos en forma de matriz, para comparar las distintas opciones el usuario utiliza una escala numérica. AHP se basa en la suposición de que los seres humanos son más capaces de hacer juicios relativos en lugar de juicios absolutos, como consecuencia de esto, el uso de la racionalidad en AHP es menor que en el caso de MAUT.
Asimismo, AHP es un proceso poco propenso a errores, permitiendo estimaciones precisas con hasta un 40% de comparaciones erróneas, a pesar de este dato, no se puede afirmar que AHP sea mejor que la estimación experta ya que está basado en comparaciones entre parejas dotándolo de una notable ventaja para los expertos, ya que resulta más práctico poder realizar comparaciones por pares que estimaciones por cada tarea.

Teniendo en cuenta que hasta la actualidad no se ha podido probar la dominación de una técnica Multicriterio respecto a las demás, en todas ellas se pueden encontrar aspectos positivos y negativos, algunos de estos están expuestos a continuación.

5.2 Comparativa

Para MAUT, sus características principales son su expresión individual de una alternativa que representa la utilidad de esta, así como que el peso de los criterios a veces es obtenido directamente. En cuanto a sus ventajas, destaca la comparación entre las alternativas de una manera más sencilla, la elección de un alternativa es transparente puesto que se elige la de mayor puntuación, se tiene en cuenta el comportamiento de varias alternativas a partir de los distintos atributos y, finalmente, como ventaja cabe destacar su rápida aplicación y en consecuencia su implementación e interpretación es más sencilla. Las desventajas que tienes es su maximización de la utilidad ya que no tiene por qué ser importante para el decisor, los pesos de los criterios obtenidos mediante preguntas a los interesados pueden no reflejar correctamente sus preferencias y finalmente, la metodología de MAUT omite algunas interacciones que pueden existir entre los diferentes atributos.

En el caso de AHP, como característica principal destaca que los pesos de los criterios y los valores de las alternativas se basan en una comparación por pares entre alternativas y criterios. Como ventajas, es una de las pocas técnicas Multicriterio que ofrece axiomas teóricos, es una de las técnicas Multicriterio que mejor comportamiento práctico tiene, proporcionando un modelo único fácilmente comprensible y flexible y que sirve para una amplia gama de problemas estructurado, proporciona una escala de medida por lo que todas las comparaciones estarán en el mismo rango, conduce a una estimación completa de la conveniencia de cada alternativa y permite seleccionar la mejor alternativa en virtud de los objetivos, la comparación por pares es más sencilla que realizar una implementación, se puede analizar el efecto de los cambios en un nivel superior sobre el inferior, da información sobre el sistema ofreciendo una vista panorámica y finalmente, permite flexibilidad para encarar cambios en los elementos de manera que no afecten la estructura total. Dentro de las desventajas presentes en este método de decisión multricriterio tenemos que los pesos obtenidos mediante las comparaciones por pares pueden no reflejar las verdaderas preferencias del usuario, los procedimientos matemáticos pueden producir resultados ilógicos y, finalmente, el problema de cambio de rango el cual consiste en la posibilidad de cambio de la ordenación inicial obtenida para las alternativas consideradas, para este problema Saaty sugiere dos tipos de situaciones: La primera es en los problemas de asignación de recursos y cuando la aparición de alguna copia introduce en el problema la idea de abundancia o escasez de una alternativa, la segunda situación, se puede considerar que la introducción de la nueva alternativa lleva asociada la incorporación al modelo de un nuevo criterio. Otra de las desventajas que se pueden encontrar en AHP es que la modelización jerárquica efectuada en AHP dado por la influencia que el número de descendientes de cada nodo tiene en la prioridad final de los elementos considerados, por ejemplo, si todas las alternativas son evaluadas en función de todos los subcriterios este problema no suele presentarse ya que cada alternativa alcanzaría su proporción que se distribuye a lo largo de la jerarquía o, si las alternativas fuesen evaluadas en función de parte de los subcriterios este problema puede afectar al resultado final, para evitar esto se sugiere efectuar un ajuste estructural de las prioridades reescalando el peso de los criterios con el número de elementos bajo el mismo.

Capítulo 6
Notorious Nine

6.1 Introducción

Para realizar el algoritmo presente en este Trabajo Fin de Grado que hace referencia a Notorious Nine se ha llevado a cabo el análisis de la lista de las nueve amenazas más importante en Cloud Computing, el propósito del informe: "*The Notorious Nine: Cloud Computing Top Threats in 2013*" [CSA] es proporcionar a las organizaciones una visión actualizada sobre las amenazas de la seguridad de la nube con el fin de realizar una gestión de riesgos de la forma adecuada y una relación correcta para manejar las estrategias de la nube. El informe de amenazas refleja el consenso entre los expertos sobre las amenazas más importantes para la seguridad de la nube.

Este informe se centra en las amenazas relacionadas específicamente con la demanda compartida de recursos en la computación de la nube. Para identificar estas amenazadas el Cloud Security Alliance (CSA) realizó una encuesta entre expertos de la industria para concentrar la opinión profesional sobre las mayores vulnerabilidades dentro de la computación en nube.

Este grupo de trabajo utilizó los resultados de la encuesta junto con la experiencia laboral y realizó este informe a finales de 2013, la metodología de la encuesta realizada valida la lista de las amenazas con las preocupaciones más actuales de la industria, en esta edición identificaron 9 amenazas críticas para la seguridad de la nube, son las siguientes ordenadas por orden de gravedad:

1. Las infracciones de datos
2. Perdida de datos
3. Secuestro de cuentas
4. APIs inseguras
5. Denegación de Servicio
6. Insiders maliciosos
7. Abuso de servicios en la nube
8. Diligencias debidas insuficientes
9. Tecnología compartida

6.2 Infracción en los datos

Es la peor amenaza posible, los datos internos de la organización caen en manos de los competidores, la computación en la nube introduce nuevas vías significativas de ataque, por ejemplo en noviembre de 2012 los investigadores de la Universidad de Carolina del Norte, la Universidad de Wisconsin y *RSA Corporación* dieron a conocer un documento que describe como una máquina virtual podría utilizar un canal lateral de información de temporización para extraer claves criptográficas privadas siendo usadas en otras máquinas virtuales con el mismo servidor físico.
Sin embargo, en muchos casos un atacante ni siquiera tendría que llegar a tales extremos. Si en una nube multiusuario su base de datos de servicio no está correctamente diseñada, un defecto en la demanda de un cliente podría permitir a un atacante acceder no sólo a los datos de ese cliente sino de otros también.

6.3 Pérdida de datos

Cualquier perdida de datos por el proveedor del servicio en la nube o cualquier otro tipo de catástrofe física, como un incendio o terremoto podría llevar a la perdida permanente de los datos de los cliente al menos que el proveedor de toma de medidas adecuada con una copia de seguridad. Por otra parte la carga de evitar la pérdida de datos hace que no caiga exclusivamente a cargo del proveedor, si un cliente encripta sus datos antes de subirlos a la nube pero pierde la clave de cifrado, los datos se perderán así quedando en manos del cliente.

6.4 Secuestro de cuentas

El secuestro de cuentas no es una amenaza nueva, ataques como el *phishing*, vulnerabilidades al fraude o explotación de software sigue siguen intentando obtener resultados. Algunas contraseñas se vuelven a utilizar amplificando el impacto de estos ataques, las soluciones de Cloud añaden una nueva amenaza para este tipo de ataque.
Si un atacante consigue acceder a sus credenciales pueden espiar sus actividades y transacciones, devolver información falsa, manipular datos o redirigir a sus clientes a sitios ilegítimos. Su cuenta o servicio puede convertirse en una nueva base para el atacante aprovechando el poder para lanzar ataques posteriores.

6.5 APIs inseguras

Los proveedores de Cloud Computing tienen un conjunto de interfaces de software o APIs que los clientes utilizan para administrar los servicios de la nube, para tener un

funcionamiento correcto hay que realizar un aprovisionamiento, gestión, orquestación y seguimiento correcto de todas estas interfaces. La seguridad y disponibilidad de los servicios de la nube dependen de estas APIs básicas.
Estas APIs necesitaran un control de autenticación y de acceso y su supervisión de actividad, tendrán por lo tanto que estar diseñadas para proteger contra ambos intentos accidentales y maliciosos de burlar la política.
Por otra parte, las organizaciones y los terceros a menudo se basan en estas interfaces para ofrecer un servicio de valor añadido a sus clientes introduciendo mayor complejidad a las nuevas APIs de capas.

6.6 Denegación de Servicio

Los ataques de denegación de servicio están diseñados para evitar que los usuarios de un servicio de la nube no puedan acceder a sus datos o aplicaciones. Siendo el servicio de la nube una víctima por consumir grandes cantidades de recursos del sistema como la potencia de procesado, memoria, espacio en disco o en red, ancho de banda…
El atacante provoca o una ralentización del sistema intolerable otorgándole un peor servicio a sus clientes.

6.7 Insiders Maliciosos

El riesgo de los insiders maliciosos ha sido objeto de debate en la industria de seguridad. Mientras el nivel de amenaza está aún en debate, la amenaza interna es el verdadero adversario.

6.8 Abuso de Servicios en la nube

Uno de los mayores beneficios de la nube de computación es que permite, incluso a las pequeñas organizaciones, el acceso a grandes cantidades de potencia de cálculo. Sería difícil para la mayoría de las organizaciones comprar y mantener multitud de servidores, pero si podían mantener miles de servidores desde una cloud computing siendo mucho más asequible.
No todo el mundo quiere utilizar este servicio para el bien, puede que un atacante rompa la clave de cifrado usando su propio hardware pero el uso de un conjunto de servidores en la nube ayudaría a realizar este proceso de una manera mucho más rápida.

6.9 Diligencias Debidas Insuficientes

Las aplicaciones CSP (política de seguridad de contenido) o servicios de la nube están siendo empujados a llevar a cabo una serie de responsabilidades operacionales tales como la respuesta a incidentes, cifrado y la supervisión de la seguridad

6.10 Tecnología Compartida

Los proveedores de servicios cloud ofrecen sus servicios de una manera escalable compartiendo infraestructura, plataformas y aplicaciones. Los componentes que conforman esta infraestructura no fueron diseñados para ofrecer fuertes propiedades de aislamiento para una multi-tenant architecture (IaaS), re-deployable platforms (PaaS), o multi-customer applications (SaaS), existe la amenaza a vulnerabilidades comunes en todos los modelos. Se recomienda una estrategia defensiva en profundidad y debe incluir computación, redes, aplicación, almacenamiento y un cumplimiento de seguridad del usuario y una supervisión de los distintos modeles IaaS, PaaS o SaaS.

Capítulo 7
Tecnologías utilizadas

7.1 Introducción

Para poder llevar a cabo este proyecto, se han usado una serie de tecnologías y herramientas donde quedan expuestas a continuación.

7.2 Estándares Web

Los estándares Web son un conjunto de recomendaciones y especificaciones técnicas generadas por el *World Wide Web Consortium* que define mejores prácticas para la construcción correcta de sitios Web. Entre los distintos estándares Web cabe destacar HTTP e Hypertext Markup Language (HTML), también, gracias al Uniform Resource Identifier podemos acceder a el recurso, para ello es necesario que este identificado de forma unívoca. El estándar URI realiza este proceso a través de una cadena corta de caracteres que puede estar formada por el domino, la ruta o el protocolo de acceso al recurso.
El lenguaje HTML puede ser creado o editado con cualquier editor de textos básico, en el caso de este proyecto con Gedit en Linux. HTML utiliza etiquetas o marcas que consisten en pequeñas instrucciones de comienzo a final, toda etiqueta se identifica por estar encerrada entre estos signos (< >), una vez se ha accedido a los datos y se transporta la información hasta el cliente, se utiliza este lenguaje para que el navegador lo interprete y pueda presentar la información.

7.3 Servlet

Un Servlet es un objeto del lenguaje de programación Java que permite la generación de contenido Web dinámico. Aunque los Servlets pueden responder a cualquier tipo de solicitud, su principal uso es extender las capacidades de un servidor Web. Para ello, se ejecutan en un contenedor Web en el servidor sin necesidad de ninguna clase de interfaz gráfica. Los Servlets cuentan con varias características que los hacen idóneos para su

utilización en servidores Web. A continuación, se citan algunas de las principales [SER07]. La primera de sus características, es su rapidez y eficiencia, los Servlets tienen una alta velocidad de respuesta debido al uso de hilos para atender a las peticiones. Además, consumen menos recursos ya que cada Servlet es cargado en memoria una sola vez en lugar de una vez por solicitud. Los Servlets pueden interactuar con otros Servlets, tanto si están situados en la misma máquina como en otra remota, lo que permite que se pueda distribuir la carga de trabajo de una misma aplicación Web entre varios Servlets mejorando los tiempos de interacción con el cliente. Al estar basados en Java, otra de sus características es su portabilidad entre plataformas, los Servlets son independientes del servidor utilizado y de su sistema operativo por cual el servidor puede estar escrito en cualquier otro lenguaje de programación. Asimismo, disponen de una API Servlet que hace más potente y sencilla su implementación, otra de sus características es que los Servlets pueden obtener información permitida por el protocolo HTTP (Hypertext Transfer Protocol) acerca del cliente. Esto junto al uso de cookies, permite el almacenamiento de dicha información dando lugar a una mejor interacción entre el servidor y el cliente donde el ejemplo más claro es el mantenimiento de sesiones. Por último cabe destacar la seguridad que proporcionan ya que al tratarse de programas ya compilados corren menor riesgo de introducir ataques de ejecución de comandos no deseados en el servidor.

7.4 Tomcat

Tomcat o también llamado Apache Tomcat, funciona como un contener de Servlets que se desarrolló bajo el proyecto Jakarta de la *Apache Software Foundation.* Funciona como contenedor web para servlets y JSPs y también puede funcionar como servidor web por sí mismo. Su jerarquía de directorios es la siguiente [Figura 8]:

- bin - arranque, cierre, y otros scripts y ejecutables.
- common - clases comunes que pueden utilizar Catalina y las aplicaciones web.
- conf - ficheros XML y los correspondientes DTD para la configuración de Tomcat.
- logs - logs de Catalina y de las aplicaciones.
- server - clases utilizadas solamente por Catalina.
- shared - clases compartidas por todas las aplicaciones web.
- webapps - directorio que contiene las aplicaciones web.
- work - almacenamiento temporal de ficheros y directorios

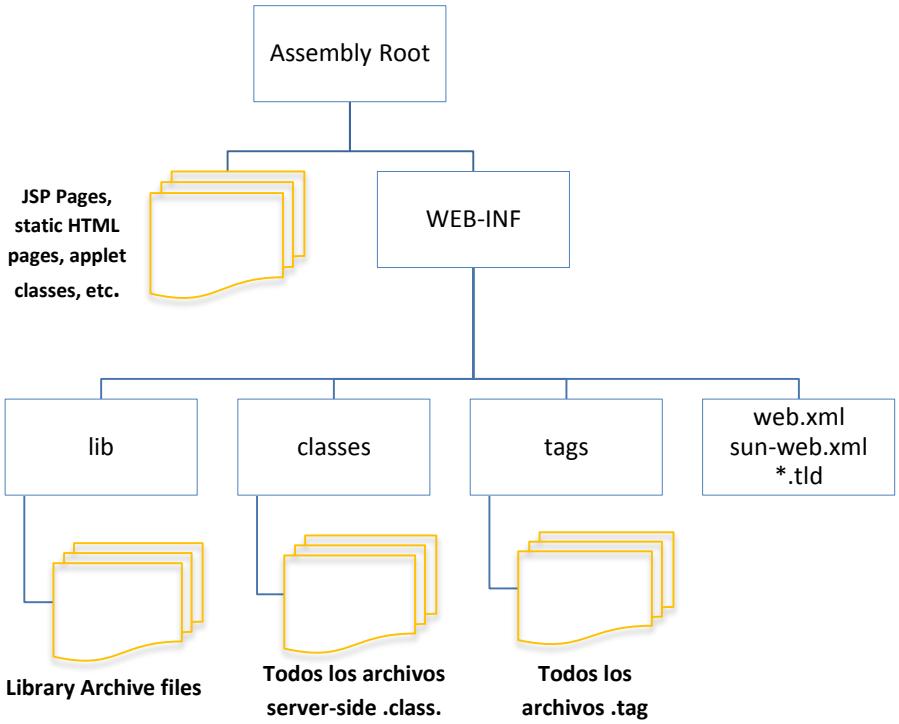


Figura 8.Directorio Tomcat

7.5 Google Charts

Dada la necesidad de presentar los datos al usuario en forma de gráficas, el desarrollador elegido para este proyecto es google. Google Chart es una API que permite, mediante una petición http, generar una imagen dinámica de tipo PNG que podemos colocar en nuestra web. Para poder crear estas gráficas, es necesario que el formato de los datos sea de un tipo determinado, para crear las gráficas del proyecto ha sido necesaria la creación de matrices para enviar los datos de forma correcta.

El origen de los datos que toma la gráfica puede provenir de distintos sitios:

- Propio código de la página HTML
- Servicio web soportado por la gráfica. (Ej.: Google Fusion, SaleForce)

Para poder mostrar las gráficas en la aplicación web, es necesario incluir tres librerías:

- La librería de la gráfica que vayamos a utilizar.
- Google JSAPI API
- Google Visualization Library

Además, dispone de un lenguaje de consulta propio, parecido a SQL, para obtener distintos datos de las fuentes, pudiendo interactuar con la gráfica. Se pueden realizar varias

modificaciones como por ejemplo añadir título, modificar los colores, grosores de líneas, pasar el cursor por encima y que aparezca un popup, etc.

Sus principales ventajas son: la gran variedad de gráficas, la presentación de los datos, posible interacción con los gráficos y su capacidad para personalizarlos. En cuando a sus inconvenientes podemos destacar: la imposibilidad de descargar el código, lo que implica la necesidad de estar conectado a Internet y la dependencia de un API externo donde cualquier variación o error no puedes controlarlo.

Algunos ejemplos de las distintas gráficas utilizadas en este proyecto son:

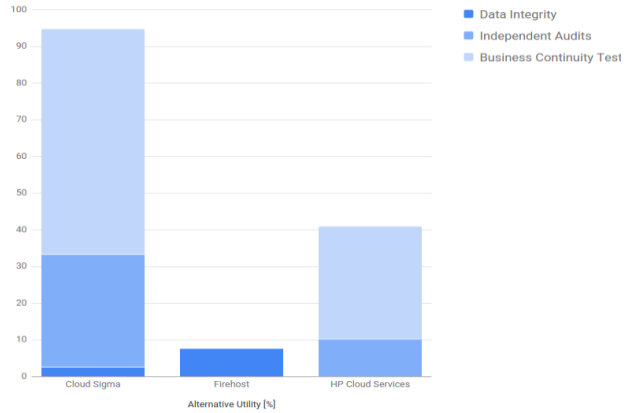


Figura 9.Gráfica de Barras

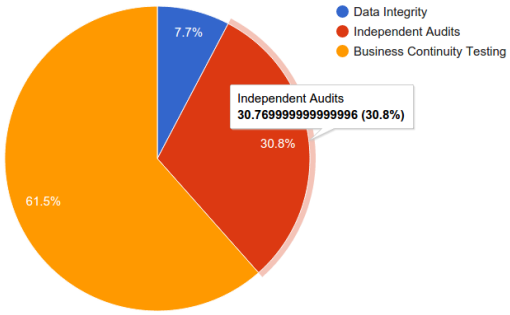


Figura 10.Gráfica de Tarta

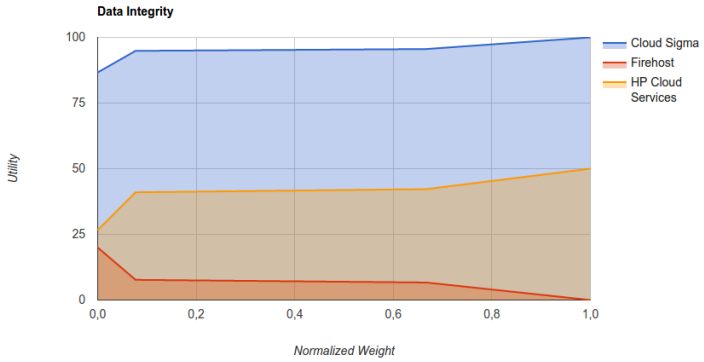


Figura 11.Gráfica de líneas

Parte III

Normativa y Marco Regulador

Capítulo 8
Normativa y Marco Regulador

8.1 Introducción

En este Trabajo de Fin de Grado se han utilizado una serie de Software de uso libre como las mencionados a continuación por lo que no se han encontrado ningún tipo de restricción para la elaboración del proyecto en función de la regulación o la normativa técnica o legal.

8.2 Apache

El uso de Apache [APA] permite al usuario la libertad para cualquier propósito, distribución, modificación y distribución de versiones modificadas del software. Sin embargo, la licencia de Apache no exige que las versiones modificadas del software se distribuyan usando la misma licencia, ni siquiera que se tenga que distribuir como software libre/open source. La licencia Apache sólo exige que se mantenga una noticia que informe a los receptores que en la distribución se ha usado código con la licencia Apache. La licencia APACHE 2.0 fue creada por la *Apache Software Foundation* (ASF), organización sin ánimo de lucro cuya finalidad es la de dar soporte al desarrollo de proyectos de software de fuentes abiertas, desde una perspectiva de hardware, de negocio y legal. Esta fundación tiene una gran importancia en el ámbito del software de fuentes abiertas, por lo que las licencias generadas por APACHE han sido utilizadas en gran número de proyectos. Existen tres versiones de la licencia: ASL 1.0, ASL 1.1 y la ASL 2.0. Desde enero de 2004, todo el software de la *Apache Software Fundation* (ASF) se publica bajo la licencia ASL 2.0. La licencia APACHE 2.0 ha sido certificada por la Open Source Initiative como licencia de fuentes abiertas.

En resumen la licencia APACHE 2.0 permite descargar y utilizar el software de Apache, en su totalidad o en parte, para uso personal, interno de la compañía, o con fines comerciales libremente; utilizar el software de Apache en paquetes o distribuciones que cree. Se prohíbe redistribuir cualquier pieza de software originado-Apache sin la debida atribución; utilizar cualquier marca propiedad de la Fundación Apache Software de sin indicar o implicar que la Fundación apoya su distribución; utilizar cualquier marca propiedad de la Fundación Apache Software de ninguna manera que pueda indicar o implicar que creó el software Apache en cuestión.

No te obligan a incluir la fuente del software Apache sí mismo, o de cualquier modificación que haya realizado a la misma.

8.3 Google

Todas las gráficas de Google [GOO] se desarrollan con privacidad y seguridad. Todas las páginas de documentación gráfica de Google incluyen una sección de política de datos que describe si un gráfico envía los datos de la página. Para la gráfica de barras como para la de tarta, que son las utilizadas en el desarrollo de este proyecto, tanto todo el código como los datos se procesan y se prestan en el navegador no se envían datos a cualquier servidor.
Por otra parte, el contenido de la página tiene la licencia *Creative Commons Atribución 3.0*, con esta licencia se es libre de compartir, es decir, copiar y redistribuir el material en cualquier medio o formato, de adaptar que indica remezclar, transformar y crear a partir del material y es tiene libre uso para cualquier finalidad, incluso comercial. Las muestras de código tienen la Licencia Apache 2.0 mencionada anteriormente.

Parte IV

Trabajo Realizado

Capítulo 9
Diseño

9.1 Introducción

En este capítulo se lleva a cabo el diseño de la aplicación web completa, se describirá el diseño de la arquitectura junto con los elementos que la componen y sus funciones, y además, se especificarán los requisitos tanto del usuario como del software.

9.2 Arquitectura

El desarrollo de la aplicación web que compone el sistema de selección de proveedores de servicios cloud basado en métricas de seguridad se ha realizado de manera progresiva siguiendo una metodología lo más dinámica posible. Por lo que, en este apartado se irán presentando la arquitectura de la aplicación junto con los elementos que la componen.

El diseño de la aplicación es el siguiente, el sistema servidor de la aplicación se compone de un servidor web, en este caso Apache, accederá al contenedor de Servlets, el contenedor de Servlets delega esta petición a un Servlet que en particular es elegido de entre todos los Servlets que contiene. El Servlet se encargará de redirigir el contenido, en el caso de esta aplicación será a un JSP obtenido de un conjunto de JSPs, finalmente, el Servlet se encargará de mostrar el contenido ya que es un objeto java y el contenedor devolverá la página web solicitada por el usuario. Entre las desventajas a destacar en el uso de JSPs, es que la carga de la interfaz es más lenta que la de una aplicación de escritorio, la mayor parte de la lógica de la aplicación se ejecuta en el servidor por lo que corre el riesgo de sobrecargarlo de trabajo o que, la aplicación puede que no esté disponible si ocurre algún problema con el servidor o con las conexión de red. En cuanto a las ventajas que presenta destaca que es un lenguaje totalmente escrito, tiene una fuerte capacidad de manipulación de gráficos, tiene cargas de APIs, es un Open Source y su ventaja fundamental es que tiene toda la ventaja del lenguaje java a nuestro alcance. Otro aspecto a resaltar de la aplicación es la integración con un servidor externo, de este servidor obtenemos metadatos que serán las meticas de seguridad de los proveedores Cloud y que serán utilizados para los cálculos.

Dentro del contenido de los distintos JSPs y Servlets, nos encontramos con cinco bloques bien diferenciados que serán utilizados para distintas funcionalidades las cuales están desarrolladas a continuación, estos bloques son: funcionalidad AHP, funcionalidad MAUT,

funcionalidad Notorious Nine, funcionalidad Gráficas y funcionalidad Parseo datos del Servidor de Metadatos externo. Finalmente, el cliente accedería a la aplicación web a través del navegador. El diseño sería el expuesto en la siguiente figura:

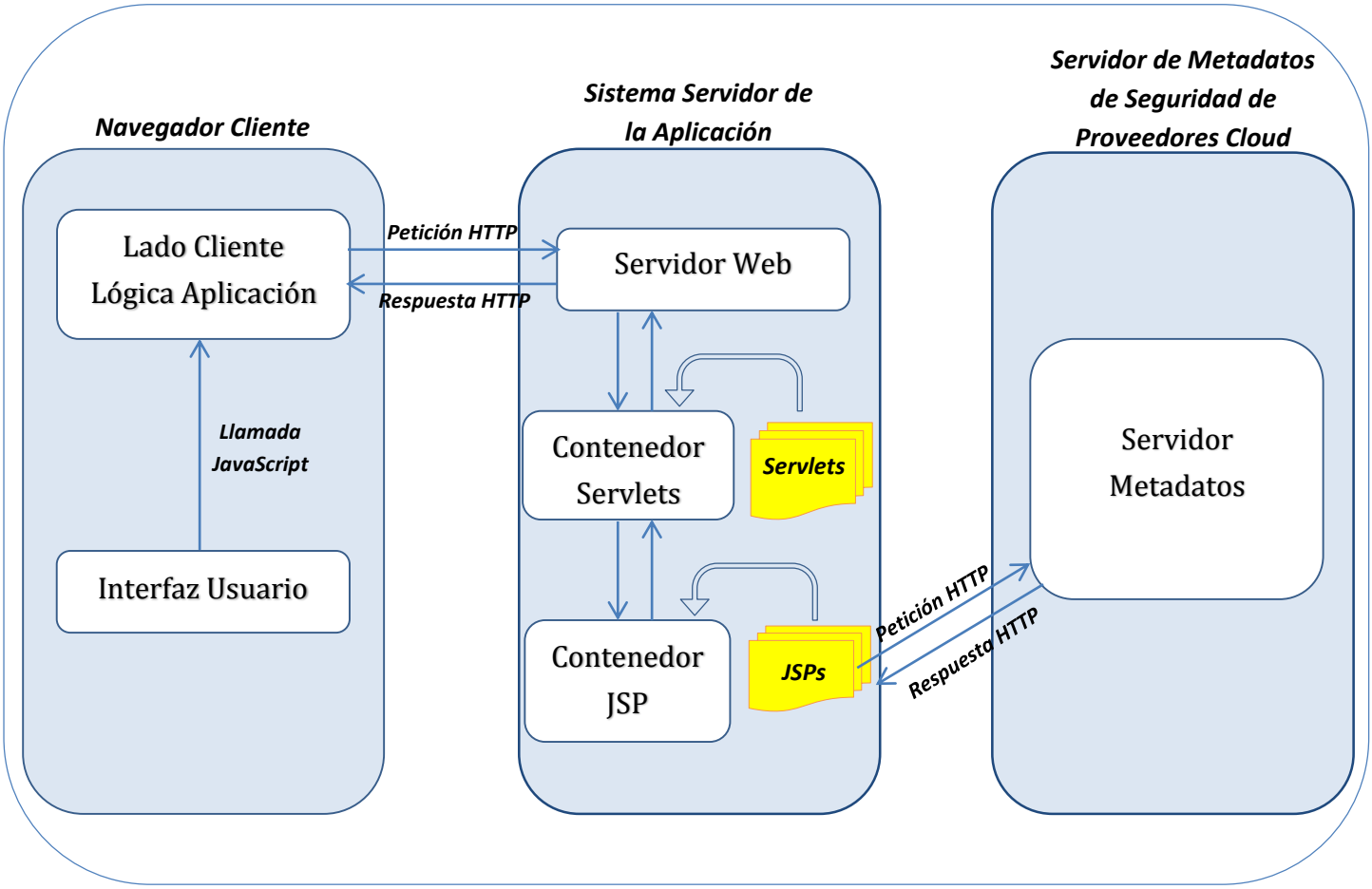


Figura 12. Diseño Arquitectura

9.3 Funcionalidad

Como ya se ha mencionado en el apartado anterior, el sistema se compone de cinco bloques con aportaciones distintas dentro de la aplicación. Como primer paso nos encontramos con la integración del servidor de metadatos externo, se trata de una API REST (REpresentational State Transfer) la cual es un tipo de arquitectura de desarrollo web que se apoya totalmente en el estándar HTTP y nos permite crear servicios y aplicaciones que pueden ser usada por cualquier dispositivo o cliente que entienda HTTP. De esta API se obtienen metadatos de los proveedores, en esta aplicación solo se implementa la comunicación con dicho servidor para así poder acceder a los datos necesarios. Estos datos se accederán a través de un servidor externo a la aplicación llamado http://jose10029.ddns.net/, al cual se accederá desde el código fuente. Esta alternativa presenta una ventaja ya que la aplicación ocupará menos que si tenemos los datos internos y también presenta la ventaja de la actualización de los datos, como desventaja principal es que el usuario debe tener acceso a internet para poder acceder a los datos, aunque esta restricción ya estaba presente.

Para la selección de criterios, a raíz de *Consensus Assessment Initiative* (CAI) la cual consiste en una iniciativa orientada a proporcionar transparencia en los servicios Cloud mediante la documentación de los controles de seguridad, esta da como resultado la creación de un documento denominado CAIQ (CAI Questionnaire) el cual se trata de un documento Excel que contiene un cuestionario, en forma de tabla, acerca de los diferentes controles de seguridad que un servicio Cloud determinado cumple, la tabla completa se encuentra en el Anexo B. Existen dos versiones del documento: la versión 1.1 y la versión 3.0.1. En este Trabajo Fin de Grado utilizaremos la versión 3.0.1.

Para la selección de proveedores, los datos son obtenidos a través del Registro de Seguridad, Confianza y Garantías (STAR) el cual es un mecanismo de certificación de proveedores Cloud a través de un registro público que contiene los controles de seguridad desarrollado por la organización CSA. Dicho registro incluye una lista de proveedores o CSP (Cloud Service Provider) cuyos documentos se encuentran publicados para la evaluación de sus servicios cloud. Los proveedores seleccionados, como primer criterio de selección está que el tipo de documento proporcionado por la empresa de ser CAI Questionnaire y, otro criterio es la versión en que se encuentran los documentos CAIQ, pueden ser en la versión inicial 1.1 y en la versión más reciente 3.0.1 puesto que la que vamos a usar es la 3.0.1 los proveedores que usaremos serán los de esa versión también.

A través de las siguientes peticiones a la API podemos consultar los siguientes datos:

- http://jose10029.ddns.net/APIREST/rest/pet/List: Mediante esta url podemos acceder a la lista de proveedores, el formato en el que se presentan los datos es JSON, en esta lista de datos obtenemos los nombres de los proveedores así como la url de la imagen, en esta aplicación la lista de 12 proveedores es:

Proveedor
Adallom
Capriza
Caretower
DataNoah
Develloc us
Everbridge
HKT
ILand
New World Telecommunications Ltd
OneLogin
Perfecto Mobile
Zscaler

Figura 13.Lista Proveedores

- jose10029.ddns.net/APIREST/rest/pet/CritNames?gran=x: Mediante esta url podemos acceder a la lista de nombre de los criterios posibles, se podrán filtran según el nivel de granularidad escogido por el usuario .El valor de la x será 1,2 o 3, siendo 1 para la granularidad baja, 2 para media y 3 para alta. Esta granularidad viene determinada

según lo expuesto en el Anexo B, la lista de "*Control Group*" corresponderá a una granularidad baja, esta lista contiene las 16 prácticas más populares para un *Cloud computing* seguro, la lista de "*Control Group ID (CGID)*" corresponde a una granularidad media, en este tipo de filtrado podemos obtener el nombre del CGID tanto de la versión 1 como el de la versión 3 que será de esencial ayuda para la implementación de *Notorious Nine* y, finalmente, la lista de "*Control Identifier (CID*)" que corresponde con una granularidad alta. La siguiente imagen muestra un ejemplo de esta estructura:

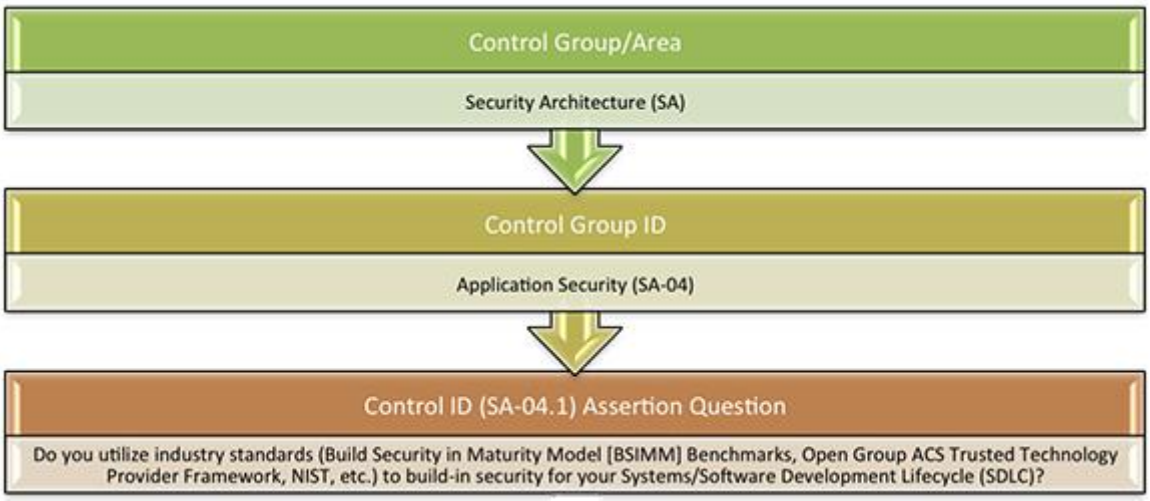


Figura 14.Organización CAIQ

- jose10029.ddns.net/APIREST/rest/pet/CritVal?gran=x: Mediante esta url podemos acceder a la lista de valores asociados a cada criterio, como en el caso anterior se podrán filtrar según el nivel de granularidad escogido por el usuario.

En la aplicación, este procedimiento correspondiente al bloque de parseo se lleva a cabo mediante AJAX y jQuery, para ello la respuesta recibida a esta petición será evaluada como JSON y devuelve un objeto JavaScript, por lo que se realiza un bucle en el cual en el caso de éxito se almacena el valor de ese JSON en una variable, una vez almacenada se procede a su parseo según sea el criterio de búsqueda deseado, por ejemplo en el caso de buscar un nombre de un proveedor dentro del JSON obtenido mediante la url "List" se pasará por parámetro un número concatenado a la palabra 'Prov' ya que como podemos observar en el siguiente fragmento de JSON (figura 15) está organizado de esa forma, una vez obtenemos los datos del servidor deseado se realizará el parseo del nombre o el logo seleccionado.


```
{
    "Prov5": {
        "name": "Devellocus",
        "logo": "http://www.devellocus.com/wp-content/uploads/2014/10/Backup_of_devellocus-logo-icon.png"
    },
    "Prov6": {
        "name": "Everbridge",
        "logo": "http://www.everbridge.com/wp-content/uploads/2014/10/hero5.png"
    },
    "Prov7": {
```


Figura 15.Formato JSON

Figura 16.Obtención metadatos

La función utilizada para obtener las métricas de seguridad en formato JSON y proceder a su parseo es la siguiente:

Nombre	jQuery.ajax([settings])
Atributos	• async: forma en la que se desea enviar las peticiones, true de forma asíncrona, false de forma síncrona. • dataType: tipo de datos que se espera recibir, en el caso de esta aplicación será JSON. • url: string con la url a donde se quiere realizar la petición.

Figura 17.Método Parseo

Otro módulo existente en la aplicación es el de gráficas, estas gráficas de Google se realizan a través de la aplicación de código HTML y JavaScript, hay dos partes bien diferenciadas para la generación de estas, primero se encuentra un el cual contiene la gráfica y segundo, el código que lo genera. Para que la gráfica se forme a través de nuestros datos, se usarán distintas variables que contendrán los datos que vayamos a usar, como por ejemplo, la gráfica de ranking final contendrá el nombre de los distintos proveedores para el eje horizontal, el nombre de cada criterio para la leyenda y el valor final asignado a cada uno de ellos correspondiente a un proveedor. Este código para generar las gráficas estará en distintos ficheros .JSP según el método que se haya seleccionado.

Por terminar con los distintos bloques que se organizan en funcionalidades, nos encontramos con AHP, MAUT y Notorious Nine, en el caso de AHP se lleva a cabo la implementación del método multricriterio correspondiente al Proceso de Análisis Jerárquico, para MAUT el método de la Teoría de Utilidad Multiatributo, y finalmente, Notorious Nine el cual se basa en la implementación del análisis de la lista de las nueve amenazas más importante en Cloud Computing, el propósito del informe: “The Notorious Nine: Cloud Computing Top Threats in 2013” [CSA] la implementación de los distintos bloques se desarrollará en el siguiente capítulo.

9.4 Diseño

El diseño final de la aplicación quedaría, una vez definidos los distintos módulos de los que se compone la aplicación como queda expuesto en la siguiente figura:

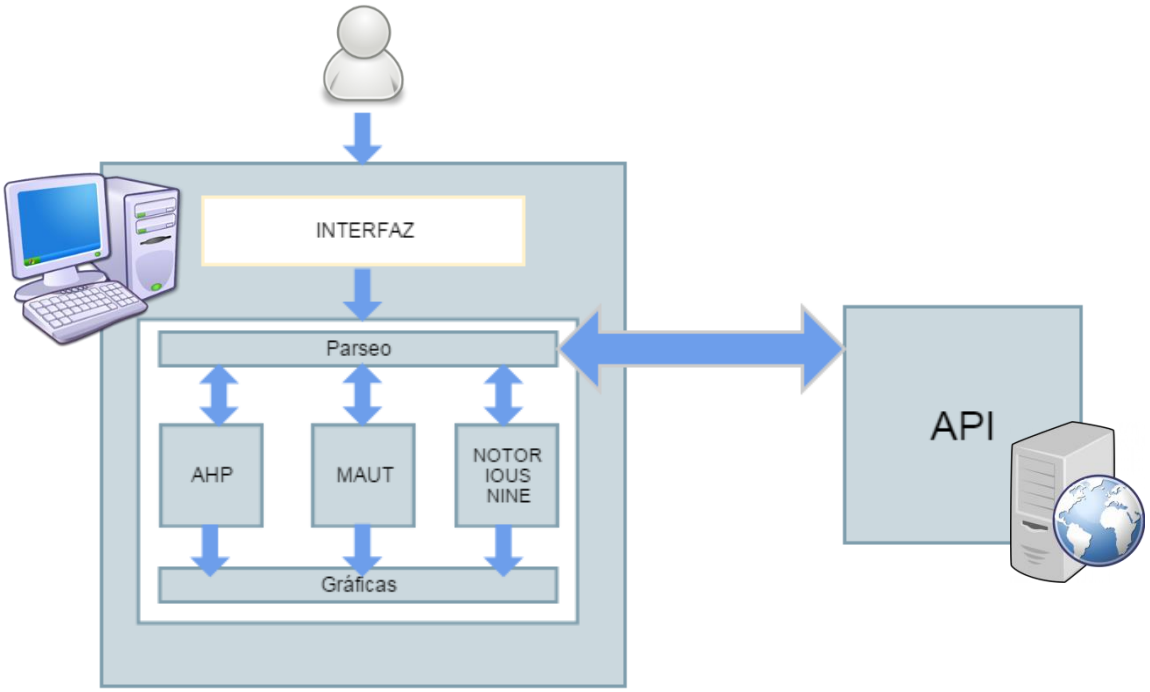


Figura 18. Diseño bloques aplicación

9.5 Requisitos

En este apartado se procede a exponer los requisitos que debe cumplir la aplicación, obtenidos a partir de las especificaciones propuestas y de las distintas limitaciones que se puedan haber presentado en su elaboración.

Los requisitos se han dividido en dos partes, por un lado, los requisitos de usuario que se dividen en requisitos de capacidad que son aquellos referidos a las acciones que puede llevar a cabo el usuario, y requisitos de restricción que son las limitaciones impuestas por el cliente, y por otro lado, los requisitos de software que se dividen en requisitos funcionales que definen el comportamiento del sistema en cuanto a las funcionalidades que se deben implementar y en requisitos no funcionales que se centran en la implementación de las funcionalidades del sistema pero imponiendo restricciones sobre los requisitos funcionales.

La especificación de los requisitos propuestos se dará mediante una serie de tablas realizadas a partir de la siguiente plantilla:

ID	RX-X
Descripción	
Necesidad	Esencial/Opcional
Tipo de Requisito	Funcional/ No Funcional
Prioridad	Alta/Media/Baja

Figura 19. Plantilla requisitos

Dónde:

- ID: indica el identificador del requisito. R [U: usuario |S: software]-[número].
- Prioridad: Puede tener tres valores y describe la prioridad del registro.
- Necesidad: Puede tener dos valores, y describe la necesidad de cumplirlo.
- Tipo de requisito: para el caso de tipo de usuario, se indica si es de capacidad o de restricción y en caso de requisito de software se indica si es un requisito funcional o no funcional.
- Descripción: incluye una descripción del requisito.

A continuación se muestran los requisitos funcionales y no funcionales siguiendo la plantilla expuesta anteriormente:

ID	RU-01
Descripción	El usuario podrá visualizar la lista de proveedores
Necesidad	Esencial
Tipo de Requisito	Capacidad
Prioridad	Alta

Figura 20.RU-01

ID	RU-02
Descripción	El usuario podrá visualizar la lista criterios
Necesidad	Esencial
Tipo de Requisito	Capacidad
Prioridad	Alta

Figura 21.RU-02

ID	RU-03
Descripción	El usuario podrá visualizar resultado método AHP
Necesidad	Esencial
Tipo de Requisito	Capacidad
Prioridad	Alta

Figura 22.RU-03

ID	RU-04
Descripción	El usuario podrá visualizar resultado método MAUT
Necesidad	Esencial
Tipo de Requisito	Capacidad
Prioridad	Alta

Figura 23.RU-04

ID	RU-05
Descripción	El usuario podrá visualizar las distintas gráficas obtenidas
Necesidad	Esencial
Tipo de Requisito	Capacidad
Prioridad	Alta

Figura 24.RU-05

ID	RU-06
Descripción	El usuario podrá seleccionar dentro de la lista de proveedores
Necesidad	Esencial
Tipo de Requisito	Capacidad
Prioridad	Alta

Figura 25.RU-06

ID	RU-07
Descripción	El usuario podrá seleccionar dentro de la lista de criterios
Necesidad	Esencial
Tipo de Requisito	Capacidad
Prioridad	Alta

Figura 26.RU-07

ID	RU-08
Descripción	La interfaz es intuitiva
Necesidad	Esencial
Tipo de Requisito	Restricción
Prioridad	Alta

Figura 27.RU-08

ID	RU-09
Descripción	La interfaz de la aplicación esta en inglés
Necesidad	Esencial
Tipo de Requisito	Restricción
Prioridad	Alta

Figura 28.RU-09

ID	RS-10
Descripción	Procesamiento JSON obtención lista de proveedores
Necesidad	Esencial
Tipo de Requisito	Funcional
Prioridad	Alta

Figura 29.RS-10

ID	RS-11
Descripción	Procesamiento JSON obtención nombre criterios
Necesidad	Esencial
Tipo de Requisito	Funcional
Prioridad	Alta

Figura 30.RS-11

ID	RS-12
Descripción	Procesamiento JSON obtención lista de valores de criterios
Necesidad	Esencial
Tipo de Requisito	Funcional
Prioridad	Alta

Figura 31.RS-12

ID	RS-13
Descripción	El sistema realizará la metodología adecuada para el cálculo de AHP
Necesidad	Esencial
Tipo de Requisito	Funcional
Prioridad	Alta

Figura 32.RS-13

ID	RS-14
Descripción	El sistema realizará la metodología adecuada para el cálculo de MAUT
Necesidad	Esencial
Tipo de Requisito	Funcional
Prioridad	Alta

Figura 33.RS-14

ID	RS-15
Descripción	El sistema realizará la metodología adecuada para el cálculo del algoritmo Notorious Nine
Necesidad	Esencial
Tipo de Requisito	Funcional
Prioridad	Alta

Figura 34.RS-15

ID	RS-16
Descripción	El sistema dispone de conexión a Internet
Necesidad	Esencial
Tipo de Requisito	No Funcional
Prioridad	Alta

Figura 35.RS-16

Capítulo 10
Implementación

10.1 Introducción

En este capítulo se va a explicar con detalle todo lo relacionado con la implementación del sistema. Para ello se van a explicar los distintos métodos implementados como son AHP, MAUT y Notorious Nine, además se acompañará con los distintos diagramas de flujo.

10.2 Implementación

Para el uso de la aplicación es necesaria una interfaz que permita la interacción con el usuario. La interfaz gráfica está formada por distintas vistas. Cada una de estas vistas se refiere a las diferentes pantallas que aparecen a lo largo del uso de la aplicación. Como primer paso para la implementación y desarrollo de la aplicación, hay una parte general que será igual para los distintos modelos de decision Multicriterio, estas vistas y sus relaciones se muestran en la Figura 47:

- **principal_layout**: En esta primera sección aparecen los distintos proveedores que, como se ha mencionado antes, se obtienen de la API a través de una consulta AJAX. A la izquierda se encuentra un menú principal el cual está aún comprimido.

- **medium_granularity:** La siguiente vista que será mostrada al usuario es la lista con los criterios de granularidad media, en esta pantalla el menú de la izquierda ya se ha descomprimido y aparecen tres botones donde se puede escoger el nivel de granularidad, en función de que botón este chequeado la visión cambiará gracias al uso de HTML DOM (Modelo de Objetos del Documento) y jQuery. Hay tres niveles posibles de granularidad: alto, medio y bajo. En el nivel bajo (low_granularity) se mostrarán los distintos Control Group, en el nivel medio (medium_granularity) para cada Control Group se mostraran distintos CGID, y en el nivel alto (high_granularity), para cada nivel de CGIDs se muestran diferentes CIDs [Anexo B], según sea este nivel de granularidad escogido, los diferentes perfiles que se pueden aplicar van a variar bloqueándose algunas opciones.

La siguiente imagen muestra un fragmento extraído del CAIQ [Anexo B] donde se puede apreciar el desglose entre los Control Groups, los CGIDs y los CIDs como muestra la figura anterior para una granularidad alta.

Control Group	CGID	CID	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1 AIS-01.2 AIS-01.3 AIS-01.4 AIS-01.5	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.

Figura 36.Fragmento CAIQ [Anexo B]

- **profile_selection:** Finalmente, una vez el usuario ha seleccionado estos dos requisitos, se seleccionará el método deseado de decisión Multicriterio que son: AHP básico, donde se le da a los criterios el mismo peso, AHP general, en el cual el usuario selecciona el valor que desea de los distintos propuestos por Saaty en una matriz donde se realiza una comparación por pares para los criterios otorgando el usuario de esa forma su propia valoración, MAUT básico como en el caso de AHP los criterios se consideraran con el mismo peso, MAUT Simplified Utility Model en este caso el vector de pesos de los criterios lo seleccionará el usuario y finalmente, la implementación del algoritmo Notorious Nine basado en el análisis de la lista de las nueve amenazas más importante en Cloud Computing, "The Notorious Nine: Cloud Computing Top Threats in 2013" **[**CSA**]** para ambos tipos de decisores. Según la granularidad escogida por el usuario, habrá modificaciones en los tipos de perfiles que se pueden seleccionar, en el ejemplo de la siguiente imagen, la granularidad escogida es la baja, por ello no se podrá seleccionar la opción Notorious Nine puesto que para proceder al cálculo necesitamos los CGID correspondientes a una granularidad media. En el caso de que la granularidad sea baja, ambos métodos tanto AHP y MAUT básico como AHP general y MAUT Simplified Utility Model pueden ser seleccionados, pero, en el caso de que la granularidad sea alta, solo se podrán seleccionar los dos tipos básicos.

Para guardar las alternativas seleccionadas en la aplicación se ha optado por almacenarlo en la sesión, para guardarlo en la sesión se usa la clase HttpSession de la Servlet API 2.0, existen APIs más actuales con servlets que vienen con la distribución J2EE, para acceder al objeto HttpSession de la sesión se accede mediante el método request.getSession(), para obtener información asociada con la sesión se usa el método getAttribute del objeto HttpSession realizando un cast al tipo de objeto apropiado y, finalmente, se usa el método setAttibute para guardar la información en una sesión.

Una vez se han explicado las distintas vistas conjuntas para todos los modelos que tiene el usuario, se explican las distintas funcionalidades implementadas a raíz de que el usuario seleccione el perfil que desea.

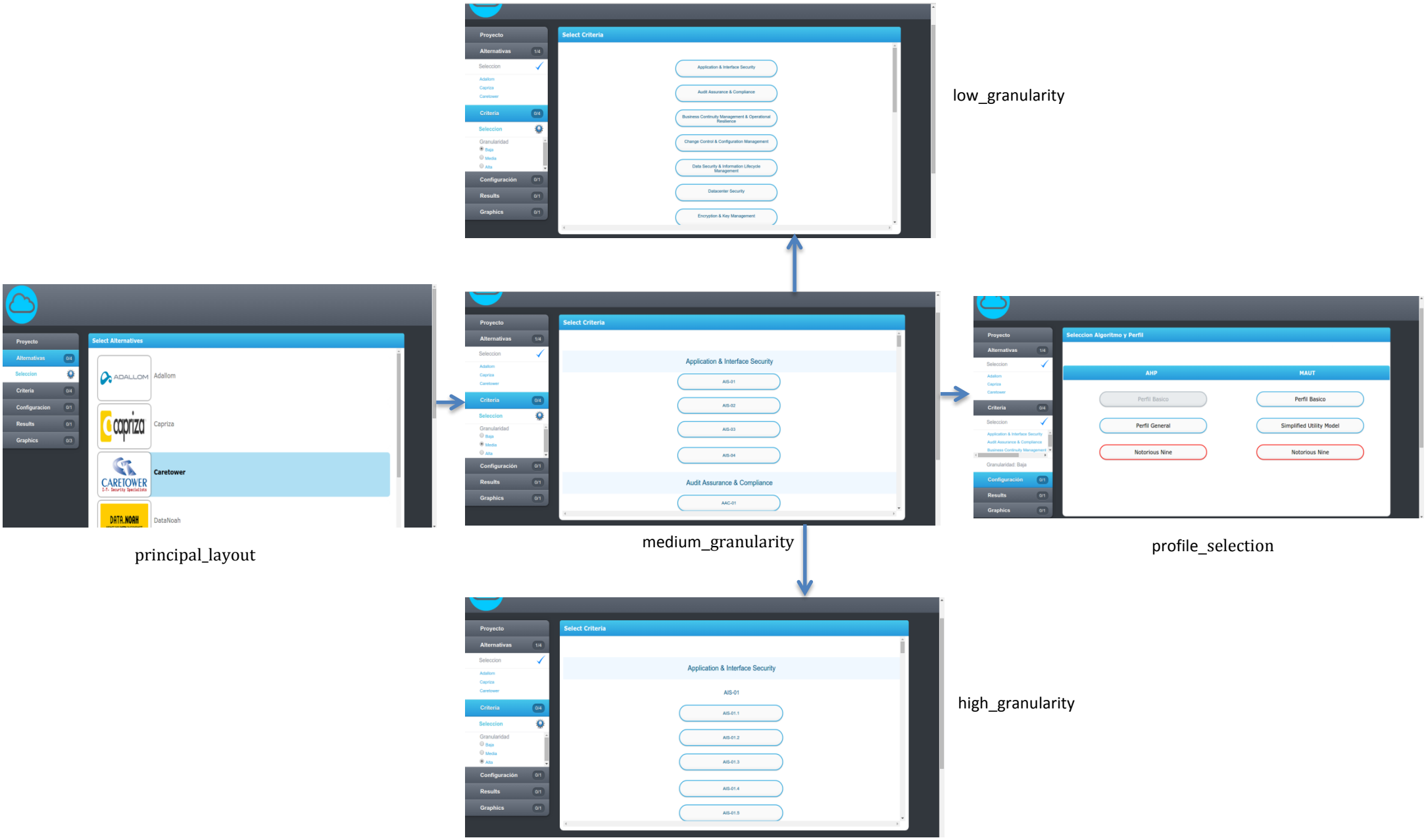


Figura 37.Vistas de la aplicación

A continuación se muestran las clases utilizadas para la implementación de los métodos, a estas clases se accederá desde los distintos JSPs. Algunos de sus métodos y atributos se explicarán más adelante.

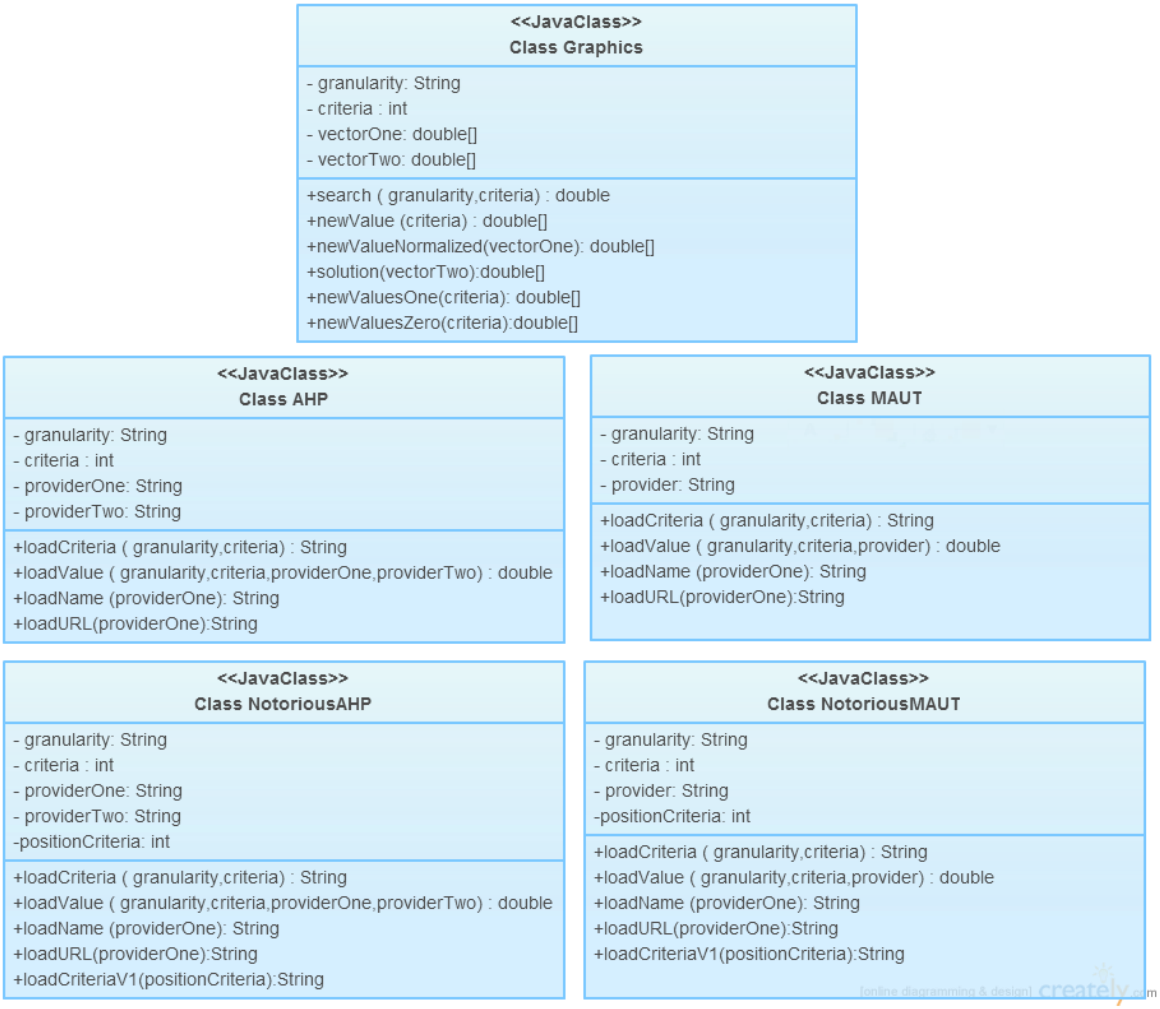


Figura 38.Clases Aplicación

Nombre	AHP
Atributos	• granularity: es de tipo String e indica la granularidad escogida por el usuario, puede tener tres valores: 'Alta', 'Media' o 'Baja'. • criteria: es de tipo Int y representa el número de criterio que se está utilizando cuando se llama al método. Según la granularidad escogida este valor será mayor. • providerOne y providerTwo: es un String y es el número de Proveedor con el cual se podrá parsear el JSON, es una cadena de tipo 'Prov' más el número.
Métodos	▪ **loadCriteria(granularity, criteria):**Es de tipo String y nos devolverá el nombre del criterio, por parámetro se le pasa el número de criterio del cual queremos obtener el nombre y el tipo de granularidad.

	▪ **loadValue(granularity, criteria, providerOne, providerTwo):** Es de tipo double y nos devolverá el valor correspondiente a los valores propuesto por Saaty [figura X], después de una comparación por pares entre los valores obtenidos para una granularidad de los dos proveedores pasados por parámetro. ▪ **loadName(providerOne)**: Es de tipo String, y nos devolverá el nombre del proveedor pasado por parámetro. ▪ **loadURL(providerOne):** Es de tipo String, y nos devolverá la url del logotipo del proveedor pasado por parámetro.

Figura 39. Clase AHP

Nombre	**MAUT**
Atributos	• granularity: es de tipo String e indica la granularidad escogida por el usuario, puede tener tres valores: 'Alta', 'Media' o 'Baja'. • criteria: es de tipo Int y representa el número de criterio que se está utilizando cuando se llama al método. Según la granularidad escogida este valor será mayor. • providerOne: es un String y es el número de Proveedor con el cual se podrá parsear el JSON, es una cadena de tipo 'Prov' más el número.
Métodos	▪ **loadCriteria(granularity, criteria):**Es de tipo String y nos devolverá el nombre del criterio, por parámetro se le pasa el número de criterio del cual queremos obtener el nombre y el tipo de granularidad. ▪ **loadValue(granularity, criteria, providerOne):** Es de tipo double y nos devolverá el valor correspondiente a un proveedor para un criterio y una granularidad dada. ▪ **loadName(providerOne)**: Es de tipo String, y nos devolverá el nombre del proveedor pasado por parámetro. ▪ **loadURL(providerOne):** Es de tipo String, y nos devolverá la url del logotipo del proveedor pasado por parámetro.

Figura 40.Clase MAUT

Nombre	**NotoriousAHP / NotoriousMAUT**
Métodos	▪ **loadCriteriaV1(criteria)**: Es de tipo String, y nos devolverá el nombre del criterio de la versión 1, pasando por parámetro su posición.

Figura 41.Clase NotoriousAHP/MAUT

10.3 AHP

En el método de AHP el primer paso consiste en realizar una jerarquía cuyo vértice superior contiene el objetivo principal o meta a alcanzar, en los niveles intermedios se representan los criterios que selecciona el usuario como se ha mencionado anteriormente (según granularidad alta, media o baja) y en la base se encuentran las distintas alternativas también seleccionadas por el usuario, un ejemplo de cómo sería una jerarquía basada en la aplicación se correspondería a la Figura 42 para una granularidad baja seleccionada, es decir, la organización según los Control Groups [Anexo B], un ejemplo de los criterios que podríamos seleccionar son "*Audit Assurance & Compliance*" o "*Business Continuity Management & Operational Resilience*" los cuales pertenecen a la columna Control Groups que contiene los diferentes grupos que engloban los controles con características comunes.

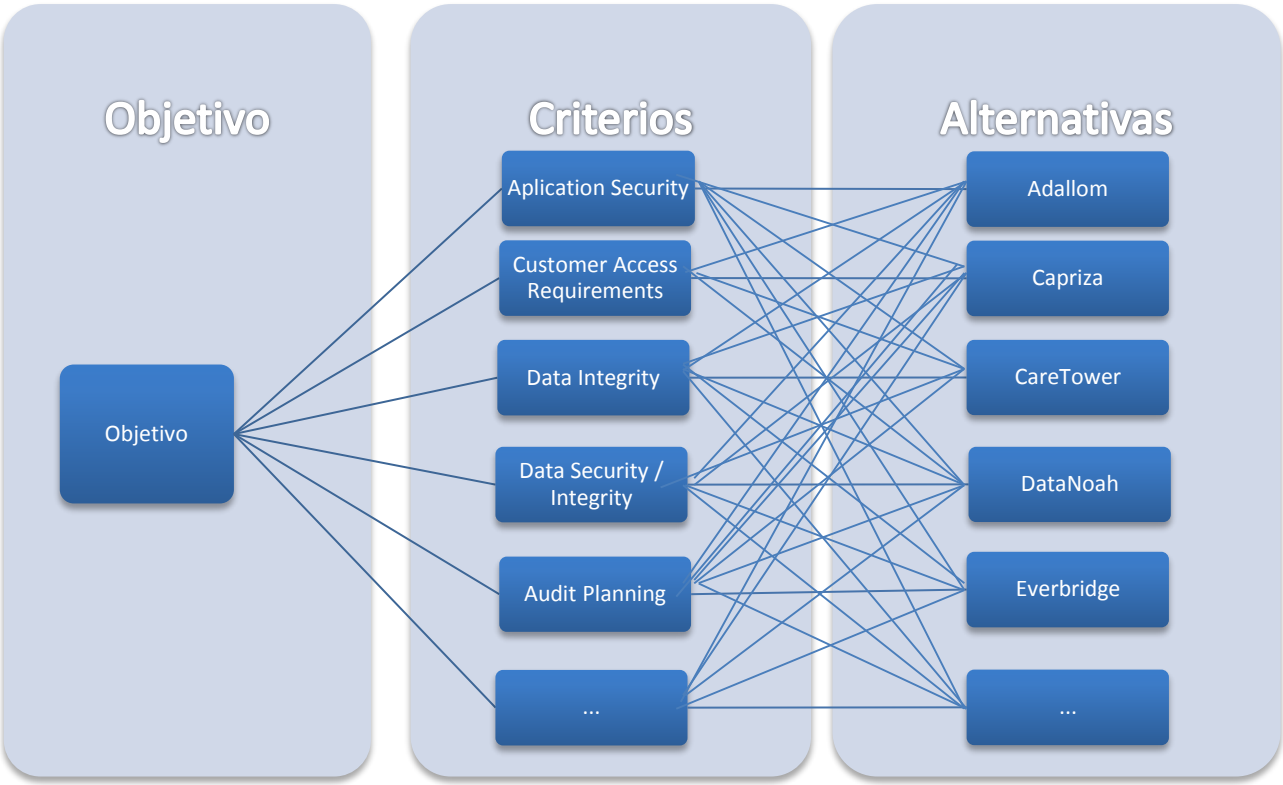


Figura 42.Jerarquia AHP de la aplicación

El conjunto de Servlets y JSPs realizados para AHP es el siguiente:

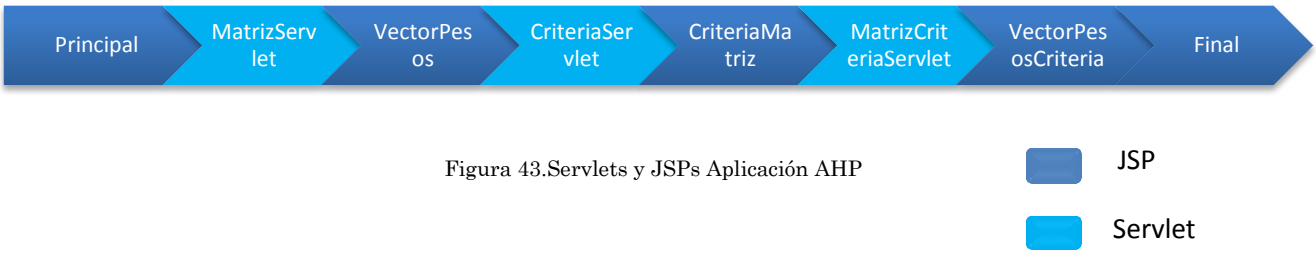


Figura 43.Servlets y JSPs Aplicación AHP

Antes de profundizar en la implementación, se muestran las distintas lógicas seguidas a partir del siguiente diagrama de flujo.

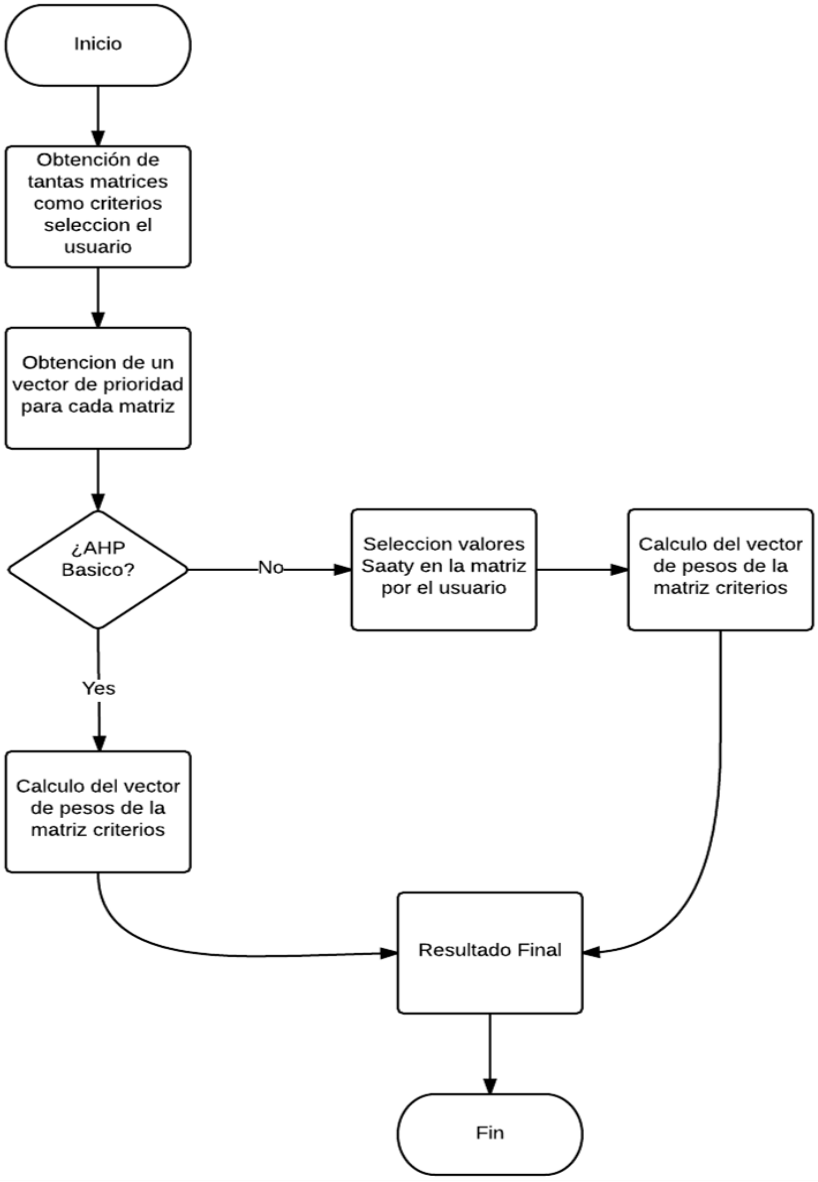


Figura 44.Diagrama de Flujo AHP

Una vez tenemos la jerarquía del modelo AHP decidida se pasa a calcular las matrices, hay tantas matrices como criterios haya seleccionado el usuario, para cada criterio se evalúan las distintas alternativas que serán los proveedores de Servicios Cloud seleccionados por el usuario, estos valores se obtienen de la API como se ha descrito en el capítulo anterior.
Los valores de la API tendrán un valor entre 0 y 1, pero, los valores que se mostrarán en la aplicación son los valores en la escala propuesta por Saaty [SAA80] en la Figura 5. Para calcular estos valores se realiza una comparación dos a dos entre las distintas alternativas para cada criterio evaluado, para ello, una vez se obtengan los valores de la API, se calculan los valores como muestra el siguiente ejemplo: si la alternativa A es 0.1 y la alternativa B es 0.5, el criterio A frente al criterio B será 1/5 mientras que el criterio B frente al A será de 5, por lo que según lo expuesto por Saaty en la Figura 5, la experiencia y el juicio favorecen fuertemente el criterio B sobre A.

Una vez obtenidas las matrices para cada criterio [Fórmula 1], se calculan los vectores de pesos de las alternativas para cada criterio, para el cálculo de estos vectores, se realiza la media geométrica y se normaliza obteniendo el vector de prioridad de las alternativas para cada criterio, continuando con este ejemplo, el proceso matemático para calcular el vector de pesos asociado por ejemplo al criterio "*Application & Interface Security*" se muestra a continuación.

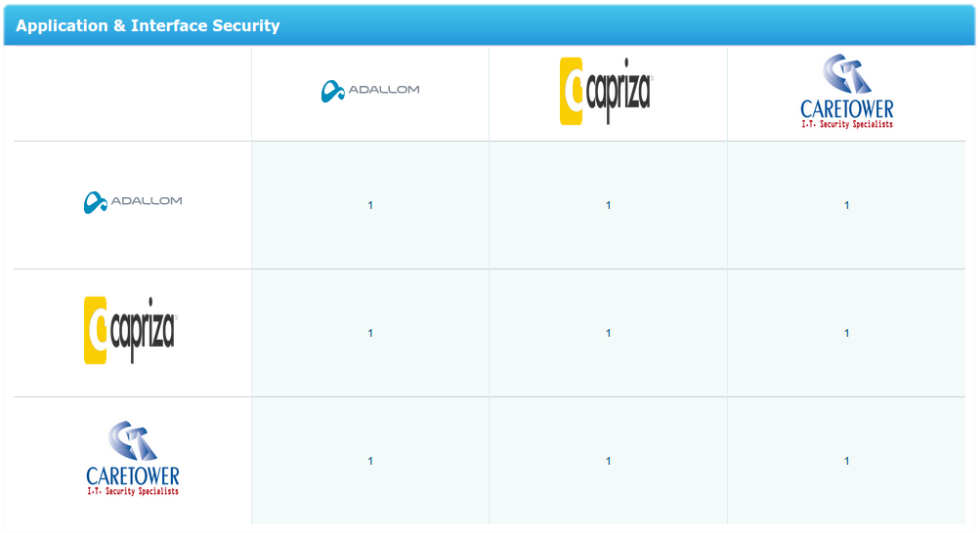


Figura 45. Matriz completa para el Criterio Application & Interface Security

$$\begin{pmatrix}1 & 1 & 1\\1 & 1 & 1\\1 & 1 & 1\end{pmatrix} * \begin{pmatrix}1 & 1 & 1\\1 & 1 & 1\\1 & 1 & 1\end{pmatrix} = \begin{pmatrix}1 & 1 & 1\\1 & 1 & 1\\1 & 1 & 1\end{pmatrix};$$

$$\begin{pmatrix}1 & + & 1 & + & 1\\1 & + & 1 & + & 1\\1 & + & 1 & + & 1\end{pmatrix} = \begin{pmatrix}3\\3\\3\end{pmatrix};$$

El vector final obtenido para el criterio "*Application & Interface Security*" el cual pertenece en la lista CAIQ a un Control Group y en la aplicación se puede seleccionar si se ha optado por una granularidad baja, es el siguiente:

$$\begin{pmatrix}\frac{3}{3+3+3} = \frac{1}{3}\\ \frac{3}{3+3+3} = \frac{1}{3}\\ \frac{3}{3+3+3} = \frac{1}{3}\end{pmatrix};$$

10.3.1 AHP Básico

Para el caso de AHP Básico, una vez obtenemos la matriz anterior hay que obtener la valoración por pares de los criterios, en el caso de AHP básico este vector de pesos tendrá el mismo valor para todos los criterios.

Para el ejemplo seleccionado el vector de pesos obtenido en la aplicación se muestra en la Figura 46. Con los distintos vectores de pesos tanto para las alternativas en función de los criterios, como con el vector de pesos normalizado obtenido de los criterios, obtenemos el vector de decision final con un valor para cada alternativa, siendo un vector de 1*n; n es el número de alternativas.

Weghts Criteria

	Application & Interface Security	Audit Assurance & Compliance	Business Continuity Management & Operational Resilience	Priority
Application & Interface Security	1.0	1.0	1.0	0.333333
Audit Assurance & Compliance	1.0	1.0	1.0	0.333333
Business Continuity Management & Operational Resilience	1.0	1.0	1.0	0.333333

Figura 46. Vector prioridad criterios AHP básico

Con el ejemplo ejecutado durante este apartado se obtendrían los siguientes datos:

Proveedor Cloud	Applications & Interface Security	Audit Assurance & Compliance	Business Continuity Management & Operational Resilience	Goal
Adallom	$\frac{1}{3} * \frac{1}{3} = \frac{1}{9};$	$0.4444 * \frac{1}{3} = 0.1481;$	$0.4 * \frac{1}{3} = 0.1333;$	0.3925
Capriza	$\frac{1}{3} * \frac{1}{3} = \frac{1}{9};$	$0.4444 * \frac{1}{3} = 0.1481;$	$0.4 * \frac{1}{3} = 0.1333;$	0.3925
Caretower	$\frac{1}{3} * \frac{1}{3} = \frac{1}{9};$	$0.1111 * \frac{1}{3} = 0.0370;$	$= 0.2 * \frac{1}{3} = 0.0666;$	0.2148
Total	$\frac{1}{9} + \frac{1}{9} + \frac{1}{9} = \frac{1}{3};$	0.1481 + 0.1481 +0.0370 = 0.3332	0.1333 + 0.1333 +0.0666 = 0.3332;	1

En la aplicación se han obtenido los siguientes datos finales:

Priority with respect to	ADALLOM	capriza	CARETOWER I.T. Security Specialists
Application & Interface Security	0.111111	0.111111	0.111111
Audit Assurance & Compliance	0.148148	0.148148	0.037037
Business Continuity Management & Operational Resilience	0.133333	0.133333	0.066667
Goal	0.39259200000000005	0.39259200000000005	0.214815

Figura 47. Resultado final AHP Básico

Las gráficas obtenidas como resultado final en la aplicación son:

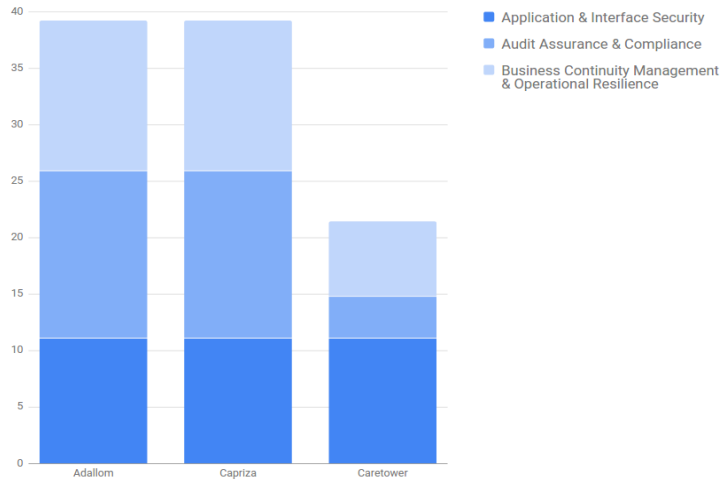


Figura 48. Gráfica AHP barras

Como se muestra en esta gráfica, y según lo obtenido en los datos, tanto Adallom como Capriza tienen la misma prioridad de 0.39259 que se distribuye en 0.11 para Application & Interface Security, en 0.14 para "*Audit Assurance & Compliance*" y en 0.13 para "*Business Continuity Management & Operational Resilience*". En el caso de Caretower la prioridad es de 0.2148 y se distribuye en 0.111 para "*Application & Interface Security*", 0.037 para "*Audit Assurance & Compliance*" y 0.0667 para "*Business Continuity Management & Operational Resilience*".

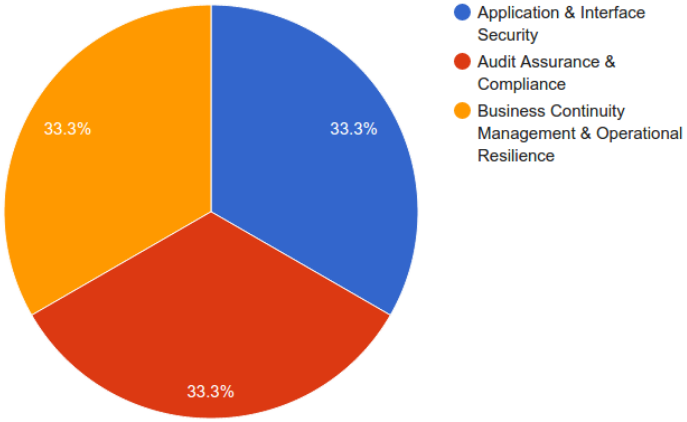


Figura 49. Gráfica Tarta AHP

En esta gráfica se muestran los pesos de los distintos criterios, en el caso de AHP Básico todos tienen el mismo peso y en este caso al ser tres el peso de cada criterio será de un tercio.

10.3.2 AHP General

Este caso varia del anterior en cómo se calcula el vector de pesos asociado a los criterios, en este caso el usuario deberá rellenar la matriz superior con los valores propuestos por Saaty [SAA80], una vez el usuario haya rellenado este matriz, la aplicación de generar la matriz completa [Fórmula 2] y generar el vector de pesos [Fórmula 3] asociado a la comparación por pares de los criterios.

Ejemplo de la matriz a rellenar por el usuario en la aplicación:

	Application & Interface Security	Audit Assurance & Compliance	Business Continuity Management & Operational Resilience
Application & Interface Security	1	9	1
Audit Assurance & Compliance	-	1	9
Business Continuity Management & Operational Resilience	-	-	1

Figura 50. Matriz AHP General Aplicación

Como en el caso de AHP Básico, con los distintos vectores de pesos tanto para las alternativas en función de los criterios, como con el vector de pesos normalizado obtenido a través del usuario, obtenemos el vector de decision final con un valor para cada alternativa, siendo un vector de 1*n; n es el número de alternativas.

10.4 MAUT

Para la ejecución correcta del método MAUT, como primer paso el decisor formula un conjunto de atributos para el problema, para cada proveedor en función del criterio se obtiene de la API un valor entre 0 y 1 el cual será representado directamente en la aplicación. El diagrama de flujo llevado a cabo para la implementación de MAUT es el siguiente:

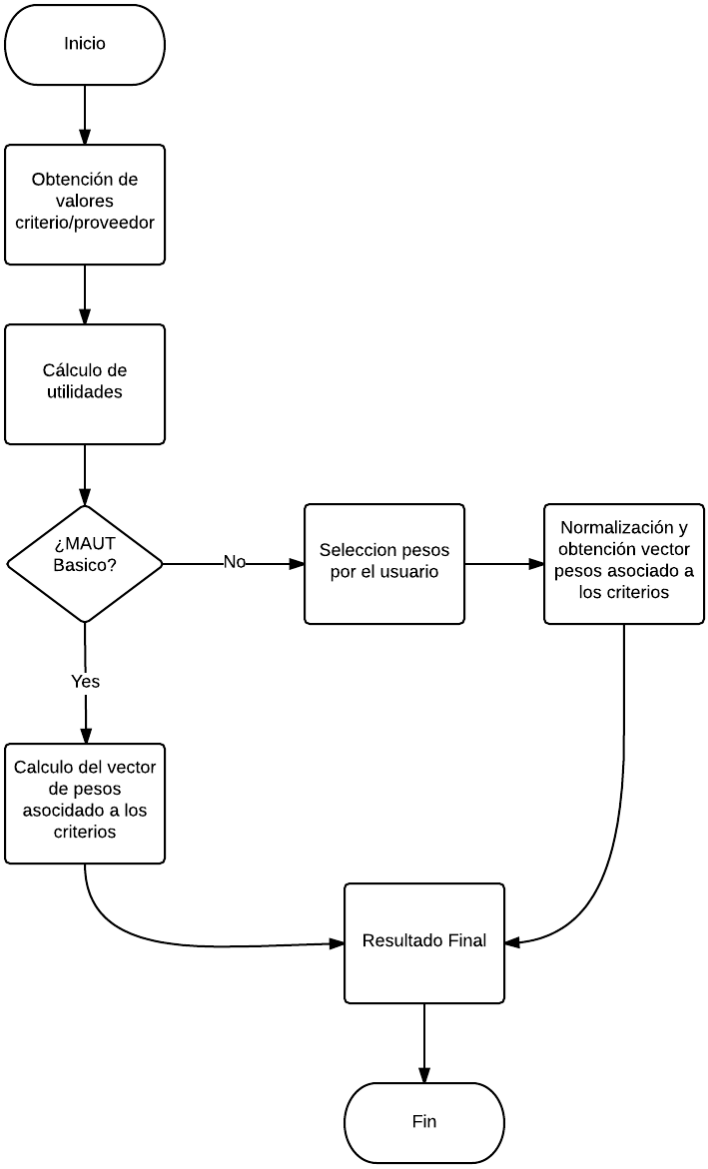


Figura 51. Diagrama de flujo MAUT

El diagrama de Servlet y JSPs propuesto en la aplicación para MAUT es el siguiente:

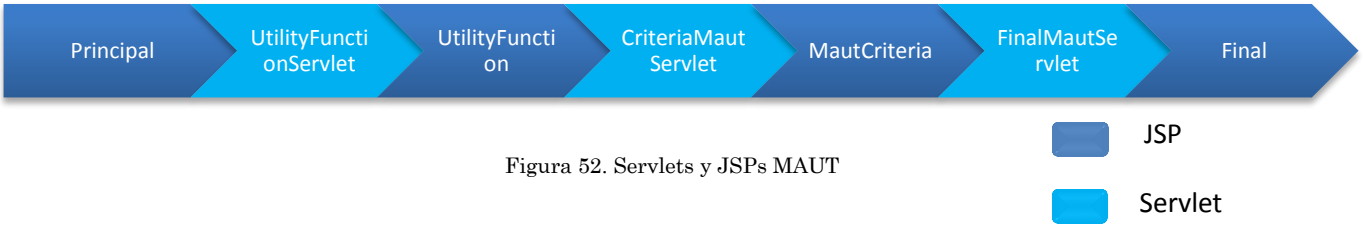


Figura 52. Servlets y JSPs MAUT

En este ejemplo se han seleccionado dos proveedores, Capriza y Caretower, y cuatro criterios, todos pertenecientes a una granularidad baja correspondiente a los Control Group de la lista CAIQ [Anexo B]:

	capriza	CARETOWER
Application & Interface Security	0.75	0.5
Audit Assurance & Compliance	1	0.8333333
Business Continuity Management & Operational Resilience	0.7818182	0.85
Change Control & Configuration Management	1	0.73333335

Figura 53. MAUT Matriz Aplicación

Una vez realizado el paso anterior, se realizará la definición de las funciones de utilidad [Fórmula 5], para cada atributo se define una función que traduce la medida evaluada anteriormente en valores de utilidad. En la aplicación obtenemos:

	capriza	CARETOWER
Application & Interface Security	1.0	0.0
Audit Assurance & Compliance	1.0	0.0
Business Continuity Management & Operational Resilience	0.0	1.0
Change Control & Configuration Management	1.0	0.0

Figura 54. Utilities MAUT Aplicación

Finalmente, se utilizan pesos para caracterizar la importancia de los distintos atributos. Estos pesos se pueden obtener mediante diversos métodos.

10.4.1 MAUT Básico

En este caso, el vector de pesos será para todos los atributos igual.

	Normalized Weight
Application & Interface Security	0.25
Audit Assurance & Compliance	0.25
Business Continuity Management & Operational Resilience	0.25
Change Control & Configuration Management	0.25

Figura 55. Vector pesos MAUT aplicación

El resultado obtenido para el caso de MAUT Básico mediante la Fórmula 9 es:

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} * \begin{pmatrix} 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \end{pmatrix} = \begin{pmatrix} 0.75 \\ 0.25 \end{pmatrix}$$

	Decision Vector
capriza	0.75
CARETOWER I.T. Security Specialists	0.25

Figura 56. Vector final MAUT Aplicación

Con este resultado obtenido, sabemos que a la hora de seleccionar un proveedor entre Capriza o Caretower para los criterios que hemos seleccionado, será una decisión mejor según lo establecido por MAUT seleccionar Capriza ya que hemos obtenido un dato tres veces mejor que para Caretower. Este dato obtenido lo podemos observar en la siguiente gráfica, donde Capriza es la mejor opción a seleccionar para un nivel global de todos los criterios, solo Caretower obtendría una mejor valoración y sería para el criterio "*Business Continuity Management & Operational Resilience*".

10.4.2 MAUT Simplified Utility Model

En este caso, la diferencia radica en la forma en la que se calcula el vector de pesos asociado a los criterios, en MAUT Simplified Utility Model el vector de pesos será seleccionado por el usuario y el valor que se le atribuye a cada criterio será entre 0 y 1, posteriormente la aplicación se encargará de normalizar este vector.

Figura 57.Simplified Utility Model MAUT vector

10.5 Notorious Nine

Para la elaboración del perfil *Notorious Nine*, se ha realizado una valoración de los criterios a través de los controles para las distintas 9 amenazas propuestas por "The Notorious Nine" [CSA].

Para llevar a cabo este procedimiento, primero se ha creado un JSON donde aparezcan los controles asociados a cada una de las 9 amenazas, por ejemplo: en la segunda amenaza propuesta "Pérdida de datos" los controles que aparecen asociados a esta son: *"CCM DG-04: Data Governance - Retention Policy"*, *"CCM DG-08: Data Governance - Risk Assessments"*, *"CCM RS-05: Resiliency - Environmental Risks*" y *"CCM RS-06: Resiliency - Equipment Location*". El nombre de estos controles son los asociados a la versión 1. El segundo paso una vez tengamos el JSON con la lista de amenazas y cada una con los controles correspondientes será realizar una petición a la API sobre los valores de los nombre de los criterios para una granularidad media. A continuación habrá que realizar un parseo de estos datos para obtener de la API el nombre asociado a la versión 1 en lugar del nombre asociado a la versión 3 que usamos en el resto de la aplicación para así poder hacer la comparación con nuestro fichero JSON cuyos datos son los de la versión 1 también.

Finalmente, habrá que a signar el valor "1" a aquellos controles de la lista CID que no aparezcan asociados a ninguna amenaza del Notorious Nine y asignar a los controles que aparecen asociados a cada amenaza valores proporcionales a la importancia de dicha amenaza, es decir, si la importancia es la 1, el valor del peso será 10, si la importancia es 2, el valor del peso será 9.

La siguiente imagen muestra lo explicado anteriormente:

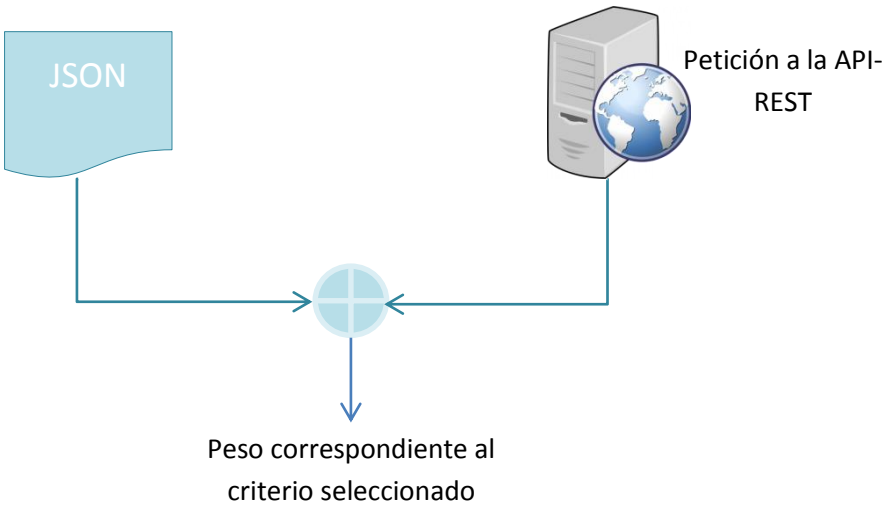


Figura 58. Obtención datos Notorious Nine

La implementación que continúa a esto es igual que la mencionada anteriormente, solo se diferencia, en el caso de AHP la comparación por pares de criterios será a través de estos valores obtenidos en el JSON, en la aplicación aparecerán directamente los valores propuestos por Saaty [SAA80] [Figura 5], es decir, se realizara la comparación entre los pesos obtenidos después de la comparación del JSON y la API entre dos criterios, si por ejemplo el valor del criterio de granularidad media “DCS-06” obtiene un peso de 8 y “DCS-07” obtiene un peso de 2, en los valores propuesto por Saaty “DCS-06” obtendría un valor de 4 frente a “DCS-07”, y “DCS-07” obtendría un valor de 0.25 frente a “DCS-06”. Una vez obtenemos la matriz se calcula el vector de pesos de los criterios [Fórmula 3].

Para MAUT se obtendrá directamente el vector de pesos sin normalizar con los valores obtenidos de los pesos obtenidos, la aplicación se encargará de normalizar este vector [Fórmula 8].El diagrama de flujo se muestra en la página siguiente.

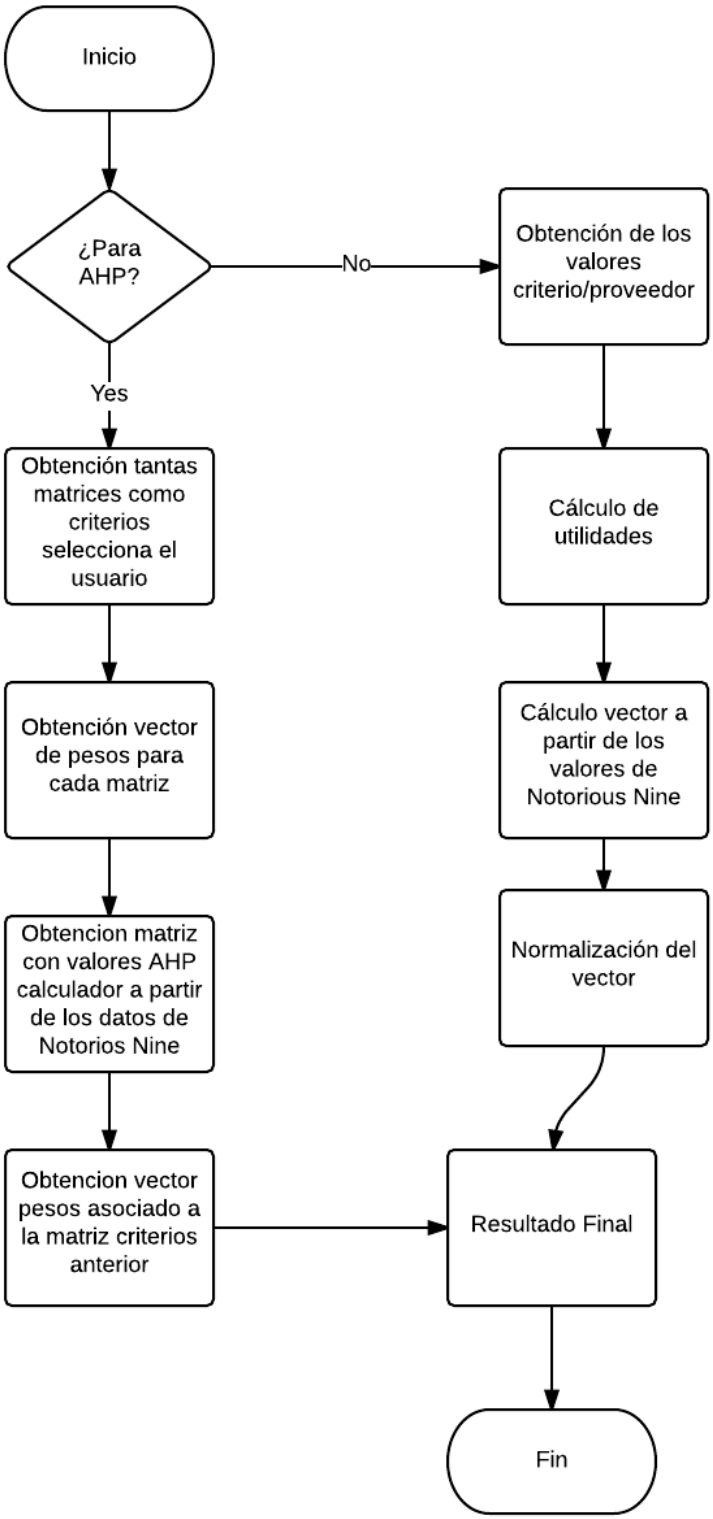


Figura 59. Diagrama de flujo Notorious Nine

Capítulo 11
Resultados

11.1 Introducción

En este capítulo se van a explicar los distintos resultados obtenidos en la aplicación de los Métodos de decision Multicriterio tanto para el caso de AHP como para MAUT , también se expondrán los resultados para Notorious Nine mediante el uso de ambos métodos multricriterio. En el caso de las pruebas realizadas para el caso de AHP y MAUT, el test se realizará con todos los proveedores, es decir 12, y para todos los criterios de granularidad baja (columna Control Group del documento CAIQ [Anexo B]) como por ejemplo el criterio "*Supply Chain Management, Transparency and Accountability*". En el caso de las pruebas realizadas para Notorious Nine (tanto para MAUT como para AHP) la lista de criterios seleccionado son aquellos pertenecientes a una granularidad media, y un ejemplo de este criterio es *"Application & Interface Security-Application Security"* el cual pertenece a la columna CGID del documento CAIQ [Anexo B], este criterio por ejemplo nos dice que las solicitudes y las interfaces de programación (API) se diseñarán, desarrollarán, instalación y prueba de conformidad con los estándares líderes de la industria (por ejemplo, OWASP para aplicaciones web) y que se adhieren a las obligaciones de cumplimiento legal, estatutarias o reglamentarias aplicables.

11.2 AHP

En este apartado se van a evaluar los resultados obtenidos con la metodología Multicriterio basado en el Proceso de Análisis Jerárquico (AHP). Como primer paso se han analizado todos los proveedores de la aplicación para todos los criterios de granularidad baja [Anexo B] es decir, los diferentes grupos que engloban los controles con características comunes, un total de 16 criterios seleccionados para los 12 proveedores cloud. La siguiente matriz de la figura 60 mide los distintos pesos evaluados donde se ha propuesto utilizar para todos los criterios la misma importancia, es decir, los mismos pesos, para este caso en concreto al tratarse de 16 posibles criterios el valor del peso de cada uno de ellos será de 1/16 es decir de 0.0625. Antes de analizar el resultado final, con los resultados expuestos en la tabla de la figura 60, podemos observar la supremacía de Perfecto Mobile e iLand así como un bajo valor obtenido por Devellocus.

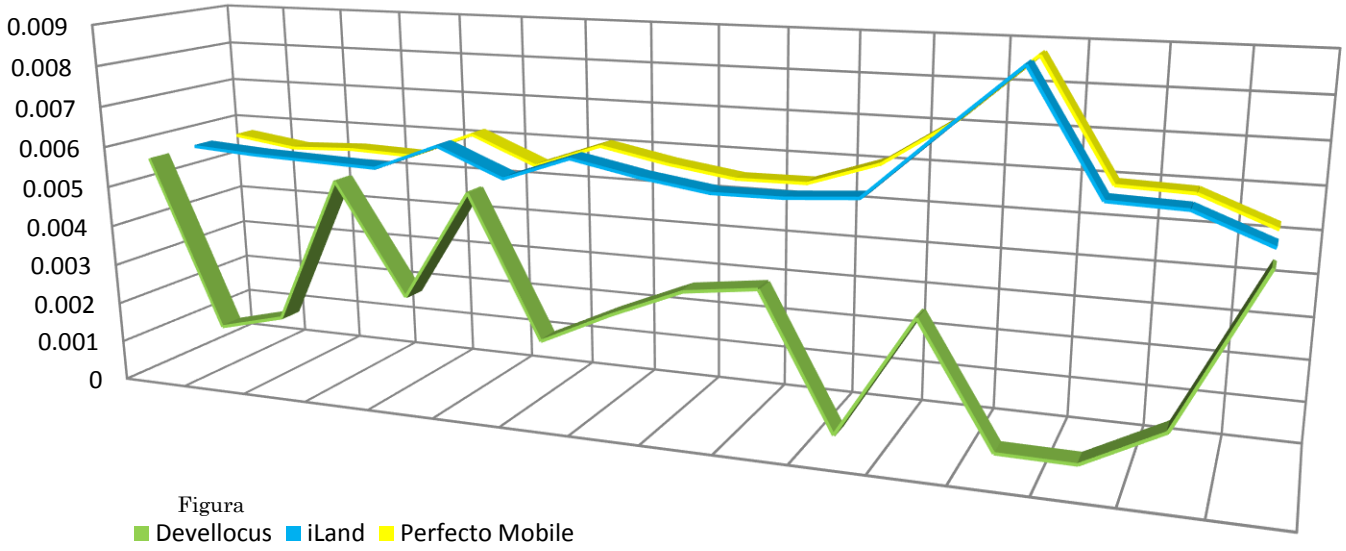
AHP

	Adallom	Capriza	Caretower	DataNoah	Devellocus	Everbridge	HKT	iLand	New World Telecommunications Limited	One Login	Perfecto Mobile	ZSCALE
Application & Interface Security	0.005685	0.005431	0.002842	0.003062	0.005685	0.005685	0.005685	0.005685	0.005685	0.005685	0.005685	0.005685
Audit Assurance & Compliance	0.005579	0.005579	0.005454	0.005579	0.001505	0.005579	0.005579	0.005579	0.005579	0.005579	0.005454	0.005454
Business Continuity Management & Operational Resilience	0.005523	0.005363	0.005523	0.005523	0.001912	0.005523	0.005523	0.005523	0.005523	0.005523	0.005523	0.005523
Change Control & Configuration Management	0.005167	0.005167	0.003573	0.005167	0.005465	0.005465	0.005465	0.005465	0.005465	0.005465	0.005465	0.005167
Data Security & Information Lifecycle Management	0.005744	0.002126	0.005565	0.005744	0.002782	0.005744	0.004549	0.006125	0.006125	0.006125	0.006125	0.005744
Datacenter Security	0.005194	0.002928	0.005438	0.005438	0.005438	0.005438	0.005438	0.005438	0.005438	0.005438	0.005438	0.005438
Encryption & Key Management	0.006045	0.006045	0.002936	0.003109	0.002049	0.006045	0.006045	0.006045	0.006045	0.006045	0.006045	0.006045
Governance and Risk Management	0.005407	0.005407	0.005407	0.003741	0.002856	0.005713	0.005713	0.005713	0.005713	0.005407	0.005713	0.005713

Human Resources	0.005167	0.005167	0.005167	0.005167	0.003573	0.005465	0.005465	0.005465	0.005465	0.005465	0.005465	0.005465
Identity & Access Management	0.005164	0.005164	0.005164	0.005164	0.003794	0.005481	0.005481	0.005481	0.005481	0.005164	0.005481	0.005481
Infrastructure & Virtualization Security	0.005606	0.005606	0.005606	0.005606	6.23E-4	0.005606	0.005606	0.005606	0.005606	0.005361	0.006061	0.005606
Interoperability & Portability	0.005617	0.002509	0.003918	0.005947	0.003493	0.00719	0.004154	0.00719	0.004154	0.004154	0.00719	0.006986
Mobile Security	0.005618	0.001793	0.008737	0.004721	6.56E-4	0.007604	0.002849	0.008737	0.007604	0.003522	0.008737	0.001922
Security Incident Management, E-Discovery & Cloud Forensics	0.005581	0.005529	0.005581	0.004013	6.37E-4	0.005581	0.00593	0.00593	0.00593	0.00593	0.00593	0.00593
Supply Chain Management, Transparency and Accountability	0.005433	0.005565	0.005433	0.003818	0.001577	0.005433	0.005874	0.005874	0.005874	0.005874	0.005874	0.005874
Threat and Vulnerability Management	0.005208	0.005208	0.005208	0.005208	0.005208	0.005208	0.005208	0.005208	0.005208	0.005208	0.005208	0.005208

Figura 60. Tabla datos AHP

Para ver los distintos resultados, se ha elaborado la siguiente gráfica con los resultados para tres proveedores, los dos con mejores resultado obtenidos (iLand y Perfecto Mobile) y el proveedor con peor resultado (Develllocus). El eje x está formado por los distintos criterios siendo cada casilla un criterio de la figura 61, en el análisis de la gráfica se puede apreciar la escasa diferencia de los resultados obtenidos con iLand y con Perfecto Mobile y la gran diferencia de ambas respecto a Develllocus.



61.Gráfica AHP

Finalmente, se evalúa el resultado final de todos los criterios para los proveedores y obtenemos los datos de la siguiente tabla, se ha remarcado en color rojo el proveedor con peores datos obtenidos, y en verde el que mejor valoración obtiene:

Proveedor	Resultado Final
Adallom	0.087738
Capriza	0.074587
Caretower	0.081552
DataNoah	0.077007
Develllocus	0.047252999999999996
EverBridge	0.09276
HKT	0.08456400000000003
ILand	0.09506400000000001
New World Telecommunications Limited	0.09089500000000002
One Login	0.08594500000000001
Perfecto Mobile	0.095394
Zscaler	0.08724100000000003

Figura 62. Tabla datos finales AHP

Según los resultados expuestos, Perfecto Mobile sería la mejor alternativa en el caso de selección de todos los criterios, a continuación con un valor muy similar, la siguiente mejor propuesta seria iLand seguida por EverBridge, NWT, Adallom y Zscaler. En la aplicación hemos obtenido esta gráfica mostrando el valor final de cada proveedor.

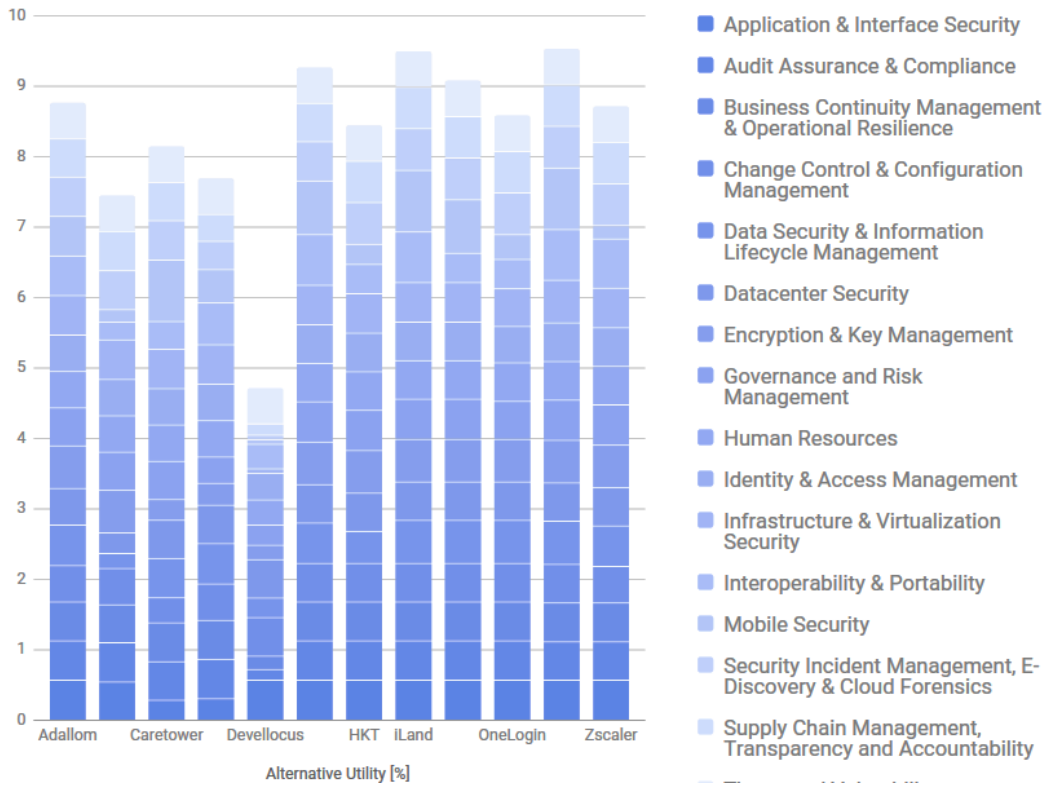


Figura 63. Gráfica barras AHP final

En la gráfica de la figura 64 aparecen representados el área de los distintos criterios para las alternativas, cabe destacar el peso de "*Interoperability & Portability y Mobile Security*" para los proveedores de servicios Zscaler, Everbridge o Perfecto Mobile. También es destacable el valor de "*Mobile Security*" para los proveedores iLand, Caretower, NWT y Perfecto Mobile.

Por todo esto, si lo que el cliente lo que desea es contratar un proveedor de servicios que ofrezca las mejores condiciones para todo los criterios seria iLand o Perfecto Mobile, en el caso de centrarse más en "*Mobile Security*", es decir, que el proveedor cumpla una conciencia anti-malware, específica a los dispositivos móviles, que el proveedor tenga una política de dispositivos móviles documentada la cual incluya una definición sobre el uso aceptable y los requisitos para todos los dispositivos móviles o que las directivas de contraseña, aplicables a los dispositivos móviles, estén documentadas y se cumplan a través de controles técnicos en todos los dispositivos de la empresa o dispositivos aprobados para el uso de BYOD (Bring your Own Device), por lo que, dentro de "*Mobile Security*", los proveedores que mejor se adaptan a el criterio son iLand, Caretower o Perfecto Mobile, en cambio, si lo que busca el cliente es un provedor que cumpla "*Supply Chain Management Transparency and Accountability*" para el proveedor deberá por ejemplo llevar a cabo evaluaciones internas anuales de conformidad y eficacia de sus

políticas, procedimientos y medidas de apoyo, o "*Threat and Vulnerability Management*" mediante la cual el proveedor deberá entre otras muchas cosas, unas políticas y procedimientos establecidos, y un apoyo a los procesos de negocio y a las medidas técnicas implementadas, para evitar la ejecución de malware en los dispositivos de punto final de usuario y de la red de infraestructura de TI , siendo en estos casos la selección del proveedor Devellocus la peor opción posible.

Figura 64. Gráfica Radar AHP final

11.3 MAUT

En este apartado se van a evaluar los resultados obtenidos con la metodología Multicriterio basado en La Teoría de Utilidad Multiatributo (MAUT). Como primer paso se han analizado, al igual que en el caso de AHP todos los proveedores de la aplicación para todos los criterios de granularidad baja [Anexo B], como ya se mencionó anteriormente, el peso de cada criterio será el mismo (al tener 16 criterios el peso de cada uno será de 1/16 = 0.0625). Según los datos obtenidos con este método podemos concluir que el proveedor más completo haciendo uso de todos los criterios es iLand seguido por Perfecto Mobile, New World Telecommunitacions Limited y EverBridge. A continuación se muestra una tabla con los valores finales obtenidos para cada proveedor, se ha resaltado en color rojo los resultados para el peor proveedor, y en verde para el caso mejor.

Proveedor	Resultado Final
Adallom	0.8299
Capriza	0.5927
Caretower	0.6516
DataNoah	0.5891
Develocus	0.2396
EverBridge	0.8848
HKT	0.8606
iLand	1.0
New World Telecommunications Limited	0.9089
One Login	0.8211
Perfecto Mobile	0.957
Zscaler	0.7247

Figura 65. Tabla resultado final MAUT

La siguiente gráfica que se muestra ha sido obtenida en la aplicación, se trata de una gráfica de barras verticales y cómo podemos apreciar destaca el bajo valor obtenido por Develocus, aún se hace más notable la diferencia con el resto de proveedores si lo comparamos con la gráfica obtenida anteriormente para el caso de AHP.

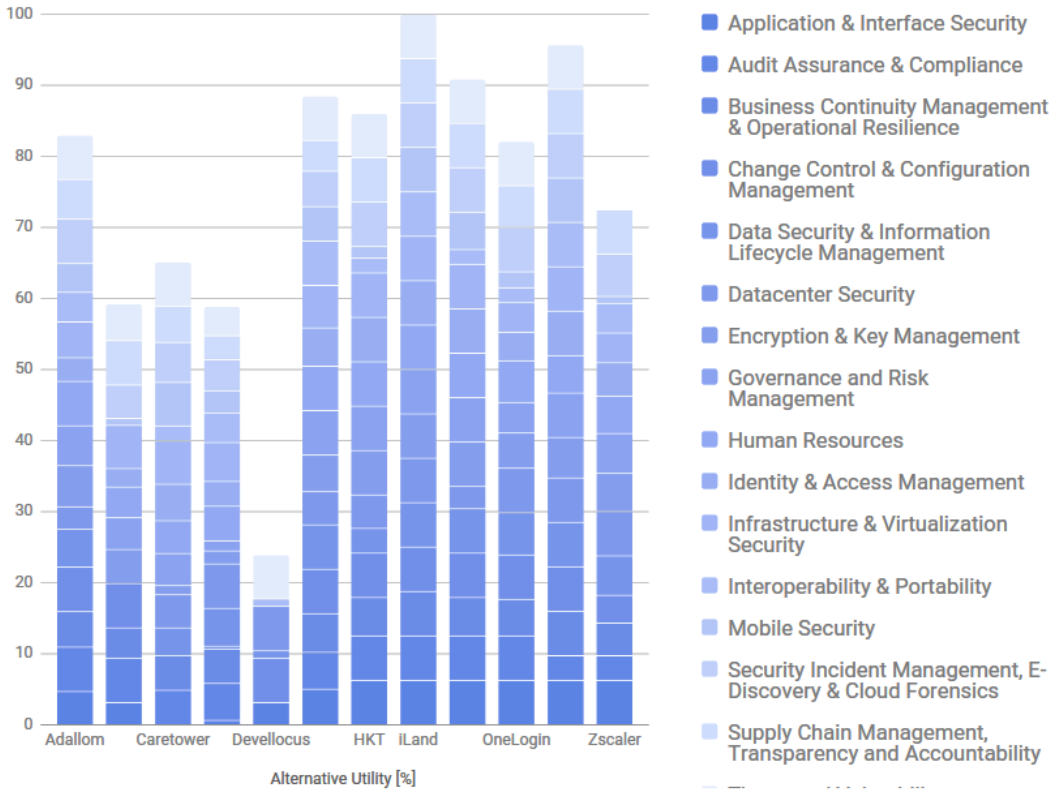


Figura 66.Gráfica barra final MAUT

En la siguiente gráfica obtenida de la aplicación, aparece representada el área de los distintos criterios para las alternativas, a diferencia del caso anterior, el área representada para cada alternativa es más equidistante para cada una de ellas, obteniendo unos pesos

similares. Como en el caso de AHP, cabe destacar los valores bajos obtenidos para Devellocus, siendo una mala elección seleccionarlo como proveedor si lo que se busca es una serie de requisitos como "*Interoperability & Portability*" o "*Mobile Security*" entre otras.

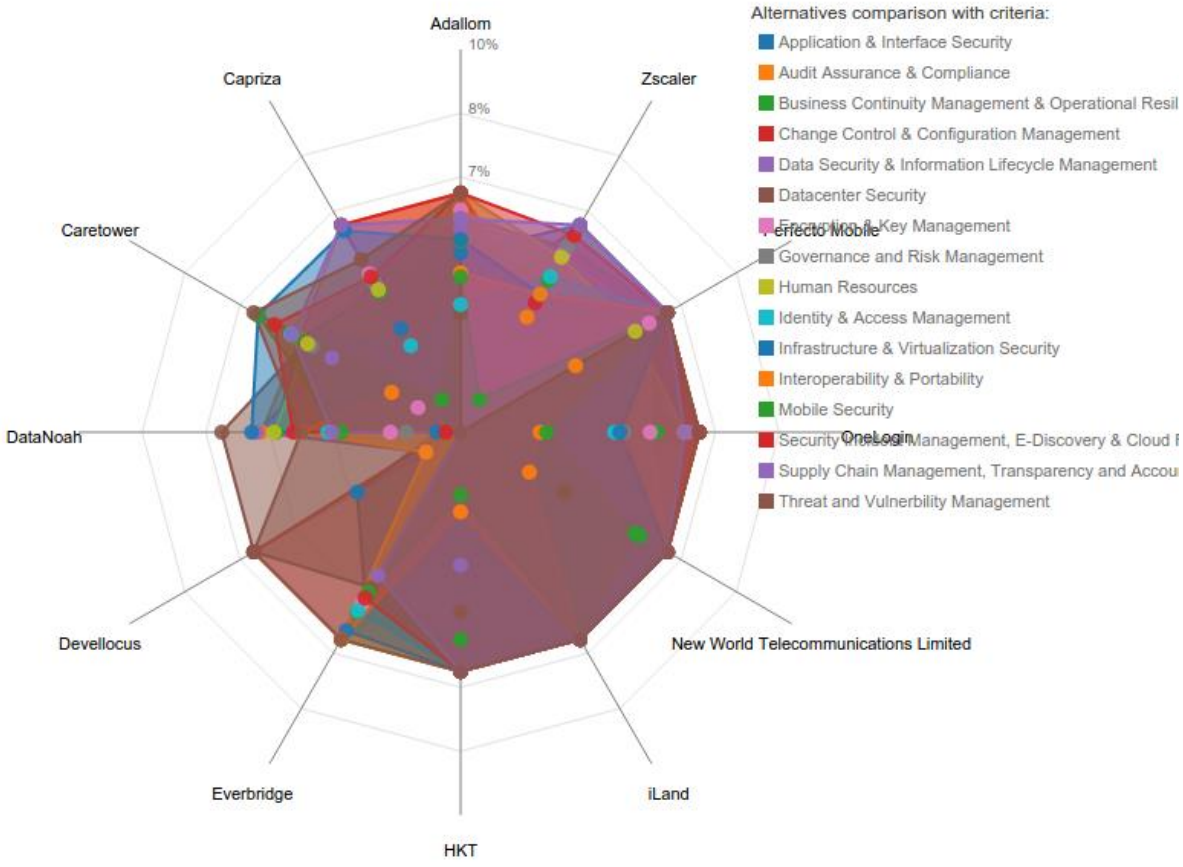


Figura 67.Gráfica Radar final MAUT

11.4 Notorious Nine

En el caso de la evaluación de proveedores en base al algoritmo de generación de pesos *Notorious Nine* se han procedido a analizar los distintos servidores de servicios Cloud en función de las Nueve amenazas definidas por el CSA [CSA] para los distintos controles asociados a cada criterio. Este análisis se llevará a cabo mediante los dos métodos de decisión implementados en este Trabajo Fin de Grado, para el caso de Notorious Nine el análisis se procede a realizar para los criterios de granularidad media puesto que como se explicó anteriormente, los controles que aparecen en la lista de las nueve amenazas son los distintos CGIDs, es decir, los identificadores de cada grupo de la lista del CAIQ [Anexo B].

11.4.1 Notorious Nine - AHP

En este apartado se llevará a cabo el análisis a través de la metodología de Proceso de Análisis Jerárquico (AHP). Los datos que se han obtenido tras la selección de todos los proveedores y los criterios de granularidad baja definidos, se ha calculado el vector de pesos final para cada criterio de granularidad media que se agrupan en una granularidad baja. Los valores para cada criterio de granularidad baja son los que se muestran en la figura 69, de los cuales podemos extraer, como hemos visto anteriormente, que los pesos más elevados para todos los criterios son los obtenidos por iLand y Perfecto Mobile salvo por una pequeña diferencia entre ambos en "*Audit Assurance & Compliance, Encryption & Key Management*", "*Human Resources*" y "*Business Continuity Management & Operational Resilience*" otorgando una ligera supremacía de Perfecto Mobile frente a iLand. También hay que destacar los bajos valores para Develloucus salvo en "*Datacenter Security*" donde obtiene una buena puntuación. Para ver los distintos resultados, se ha elaborado la siguiente gráfica con los resultados para tres proveedores, los dos con mejores resultado obtenidos (iLand y Perfecto Mobile) y el proveedor con peor resultado (Develloucus). El eje x está formado por los distintos criterios siendo cada casilla un criterio, en el análisis de la figura se puede apreciar la escasa diferencia de los resultados obtenidos con iLand y con Perfecto Mobile y la gran diferencia de ambas respecto a Develloucus que queda remarcada en la gráfica para las columnas número 13 y 14 perteneciente a los criterios "*Mobile Security*" y "*Security Incident Management, E-Discovery & Cloud Forensics*" respectivamente donde Develloucus obtiene una puntuación de 0.019671 y 0.011707 y iLand y Perfecto Mobile una puntuación de 0.128032 y 0.09759599999999999.

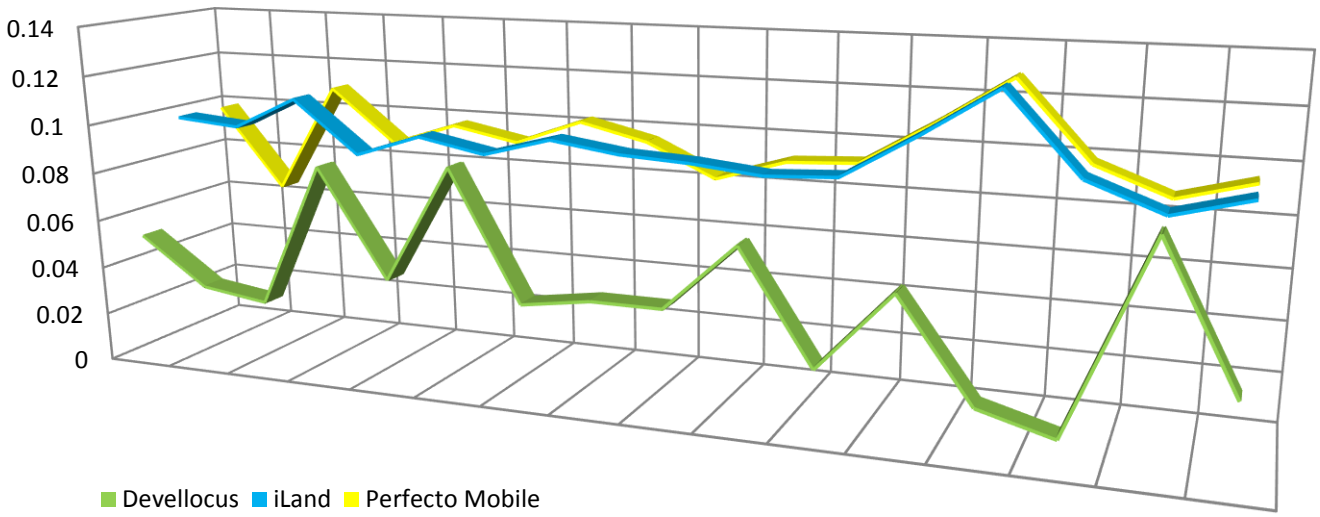


Figura 68.Gráfica Notorious AHP

AHP-Notorious Nine

	Adallom	Capriza	Caretower	DataNoah	Devellocus	Everbridge	HKT	iLand	New World Telecommunications Limited	One Login	Perfecto Mobile	ZSCALE
Application & Interface Security	0.095946	0.0934850000000001	0.062324000000000004	0.023009	0.052917000000000006	0.082606	0.0982860000000001	0.0982860000000001	0.0982860000000001	0.0982860000000001	0.0982860000000001	0.0982860000000001
Audit Assurance & Compliance	0.095989999999999	0.095989999999999	0.092219	0.081061000000001	0.033525	0.08189	0.095989999999999	0.095989999999999	0.095989999999999	0.095989999999999	0.064669	0.070692
Business Continuity Management & Operational Resilience	0.070719	0.098439	0.071066	0.072185	0.02965	0.078562	0.082509	0.10910799999999998	0.087364	0.092599999999999	0.10958399999999999	0.098215
Change Control & Configuration Management	0.086847000000000001	0.086847000000000001	0.062926000000000001	0.070356	0.08777	0.08777	0.08777	0.08777	0.08777	0.08777	0.08777	0.078650000000000001
Data Security & Information Lifecycle Management	0.095188	0.039295	0.067705999999999999	0.082293	0.044521	0.096856	0.091260000000000001	0.096856	0.096856	0.096856	0.096856	0.095466
Datacenter Security	0.081664	0.054754	0.069151	0.091524	0.091524	0.08791	0.087163999999999999	0.091524	0.070204	0.091524	0.091524	0.091524
Encryption & Key Management	0.090205	0.080568	0.049357000000000005	0.069184	0.040081	0.094223999999999999	0.099117	0.099117	0.099117	0.090428	0.101697	0.086904

Governance and Risk Management	0.0801670000000002	0.0849940000000001	0.0848810000000001	0.065441	0.04423	0.095188	0.095188	0.095188	0.095188	0.0817079999999999	0.095188	0.082645
Human Resources	0.0933899999999999	0.069064	0.0792939999999999	0.0813909999999999	0.044152	0.0936769999999998	0.0936769999999998	0.0936769999999998	0.0936769999999998	0.0936769999999998	0.0821689999999999	0.0821689999999999
Identity & Access Management	0.0792320000000001	0.0742959999999999	0.0817820000000001	0.068022	0.0708019999999999	0.084635	0.090809	0.090809	0.090809	0.0883799999999999	0.090809	0.089625
Infrastructure & Virtualization Security	0.080969	0.09135	0.0914649999999999	0.088772	0.02715	0.082611	0.092303	0.092303	0.092303	0.0832229999999999	0.092303	0.085238
Interoperability & Portability	0.087777	0.044066	0.062995	0.088322	0.058639	0.109459	0.074479	0.109459	0.0848770000000001	0.074657	0.109459	0.095808
Mobile Security	0.083083	0.025754999999999993	0.125798	0.067081	0.019671	0.1021829999999998	0.0546829999999999	0.128032	0.1127680000000001	0.0783459999999999	0.128032	0.0745940000000001
Security Incident Management, E-Discovery & Cloud Forensics	0.097595999999999	0.073291	0.071504	0.090045	0.011707	0.070285999999999	0.097595999999999	0.097595999999999	0.097595999999999	0.097595999999999	0.097595999999999	0.097595999999999
Supply Chain Management, Transparency and Accountability	0.084719999999999	0.0847199999999999.101154	0.084719999999999	0.070178999999999	0.086957	0.086957	0.086957	0.086957	0.086957	0.086957	0.086957	0.066957
Threat and Vulnerability Management	0.088061	0.0946320000000001	0.0825060000000001	0.0631680000000002	0.032869999999999996	0.0743600000000001	0.0946320000000001	0.0946320000000001	0.0946320000000001	0.091252	0.0946320000000001	0.0946320000000001

Figura 69. Tabla datos Notorios Nine AHP

11.4.2 Notorious Nine - MAUT

En este apartado se llevará a cabo el análisis a través de la metodología de La Teoría de Utilidad Multiatributo (MAUT). Los datos que se han obtenido tras la selección de todos los proveedores y todos los criterios para una granularidad media son los siguientes:

Proveedor	Resultado Final
Adallom	0.8708
Capriza	0.7266
Caretower	0.7663
DataNoah	0.6786
Develloucus	0.3647
EverBridge	0.866
HKT	0.9183
ILand	0.9969
New World Telecommunications Limited	0.9406
One Login	0.8727
Perfecto Mobile	0.9871
Zscaler	0.8592

Figura 70. Tabla final Notorious Nine MAUT

Como podemos observar, tras el análisis de Notorious Nine para MAUT el proveedor que más peso obtiene es iLand seguido por Perfecto Mobile con un bajo margen, el siguiente proveedor que obtiene una buena puntuación es New World Telecommunications Limited y HKT. El proveedor que menor valor obtiene, tal como se vio en los resultados anteriores es Develloucus.

11.5 Conclusión

Como conclusión principal para el caso del análisis mediante los métodos de decisión Multicriterio para el caso del Proceso de Análisis Jerárquico (AHP) y el de la Teoría de Utilidad Multiatributo (MAUT) destaca el alto valor obtenido para los proveedores de servicios Cloud iLand y Perfecto Mobile para los distintos criterios, también hay que destacar el bajo valor obtenido con ambos decisores Multicriterio para el proveedor Develloucus, siendo aún más notable la diferencia de valor respecto al resto de proveedores utilizando MAUT.

También hay que destacar el alto valor obtenido para ambos casos de metodologías de los proveedores EverBridge o New World Telecommunitacions Limited, siendo también una buena opción.

En el caso del análisis de Notorious Nine también obtenemos unos datos parecidos a los obtenidos en los casos anteriores, siendo iLand y Perfecto Mobile los proveedores más importantes y Develocus el que obtiene peor valoración.

Según las distintas formas que puede adoptar la nube, los proveedores utilizados en este análisis, se pueden dividir en:

- **Infraestructure as a Service (IaaS):** En este caso se contrata la capacidad de proceso (CPU) y el almacenamiento. En este entorno se pueden desplegar aplicaciones propias que por motivos de falta de conocimiento o de coste no queremos instalar en nuestra propia empresa, por lo que, el proveedor se encarga de su gestión, convirtiéndose así todos los gastos en variables para el cliente, es decir, solo se paga por lo que se usa.

- **Software as a Service (SaaS):** En este caso es una aplicación para el usuario final donde se paga un alquiler por el uso del software. En este caso no es necesario adquirir un software en propiedad, instalarlo, configurarlo o mantenerlo. En este tipo de servicios nosotros accedemos normalmente a través del navegador sin atender al software. Todo el desarrollo, mantenimiento, actualizaciones, copias de seguridad es responsabilidad del proveedor. El software as a Service está experimentando un rápido crecimiento en los últimos tiempos.

- **Platform as a Service (PaaS):** se proporciona además un servidor de aplicaciones y una base de datos. Pudiendo instalar las aplicaciones y ejecutarlas. Es un modelo que reduce bastante la complejidad a la hora de desplegar y mantener aplicaciones ya que las soluciones PaaS gestionan automáticamente la escalabilidad usando más recursos si fuera necesario.

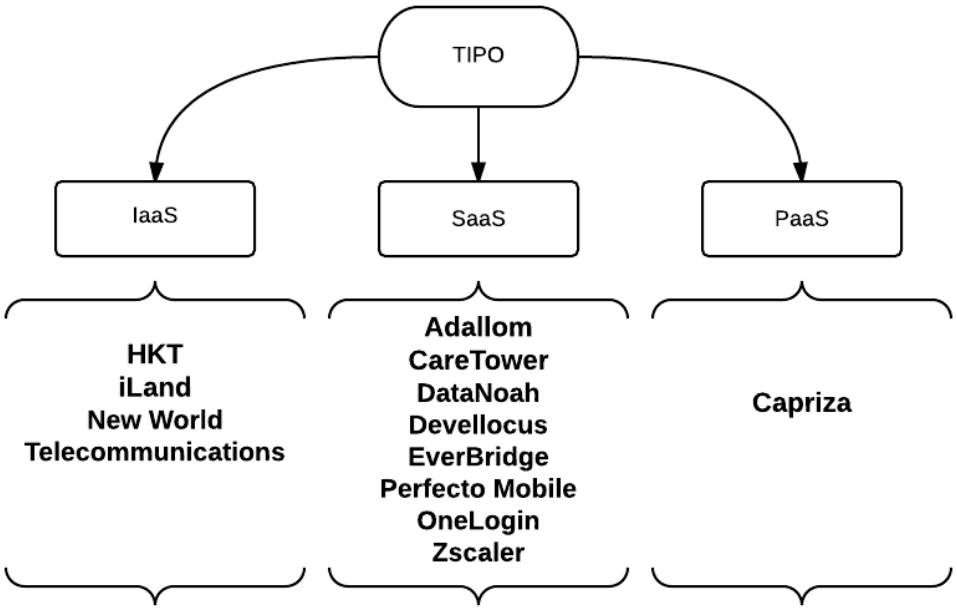


Figura 71. Listado de Servidores en función del tipo de servicio Cloud

Una vez diferenciado los distintos proveedores, como se indicó anteriormente, el tipo SaaS está experimentando un gran aumento en los últimos años, y queda reflejado en que la mayoría de los utilizados en este Trabajo Fin de Grado pertenecen a este grupo. Por otro lado, los resultados obtenidos para el grupo IaaS son buenos ya que todos los proveedores que lo componen no han obtenido malos resultados, en el caso de SaaS, en este grupo se encuentra uno de los mejores proveedores como es Perfecto Mobile pero también se encuentra Develllocus el cual obtuvo malos datos, finalmente, de tipo PaaS solo nos encontramos con Capriza. Para analizar numéricamente los datos obtenidos, se han calculado las medias de los pesos obtenidos para cada tipo de proveedor, las medias son:

- AHP :
    - IaaS: 0,09017433.
    - SaaS: 0,08186125.
    - PaaS: 0.074587.
- MAUT :
    - IaaS: 0,92316667.
    - SaaS: 0,712225.
    - PaaS: 0.5927.

Con estos datos obtenidos podemos concluir que el tipo de Cloud que mayor valor obtiene es el IaaS con una puntuación media muy alta, seguido por el tipo SaaS y finalmente el grupo PaaS el cual solo estaba formado por Capriza, hay que destacar el valor medio tan distante entre el tipo de Cloud IaaS y el tipo PaaS, que llega a ser de un 36% para MAUT.

Part V

Conclusion

Chapter 12
Conclusions and Future Work

12.1 Introduction

In this chapter of the report we expose the personal final conclusions of the project and we will come up with possible future lines that could be followed from this work.

12.2 Conclusions

The aim of this final project was to study the different types of multicriteria decision to give a business approach, in this case to the decision of various cloud service providers based on various security metrics. From the point of view of the MCDM there is no doubt that many of the problems of real life can be treated as such problems, and we can say that the decision has always been present in many ways to throughout history evolved into making decisions based on the study, analysis and reasoning of the information they possess.

With respect to the web application that has been developed, my level of satisfaction is high because I believe that the objective of this Final Project is very interesting and useful. Also the study of different methods can be used for multiples projects in future because I consider them very useful and can be set for many problems, for example, from a selection of a logistics operator with which to form a strategic alliance to a selection for a new location for building up.

As for the few difficulties presented in the project, it is noted the little existence of material of decisions applications based in Multicriteria but especially developed with Multi Attribute Utility Theory (MAUT).

The conclusions drawn from the resolution of this project and with the study of the methods of decision making based on multiple criteria can be deducted once seen the results obtained in the application that for MAUT the main aim of the decision maker is to maximize the utility value so that in the event that some criteria with low weight, can be compensated by high scores on other criteria, on the other hand, there is subjectivity when comparing both methods but after assessing the results, selecting preferences a supplier were similar because it was the same for both methods decider.

Moreover, the processing time with AHP is much higher than in the case of MAUT because AHP needs to perform pairwise comparisons of Suppliers for N criteria selected in each case. To MAUT this time is reduced because the values are obtained directly without peer comparison between them.

As the results, as mentioned above, both methods obtain a similar result, in the case of AHP this method obtains a higher value for the cloud service provider Perfect Mobile against iLand but they are very similar, and in the case of using MAUT is iLand which obtains a higher value against Perfecto Mobile, then both methods that have a similar value are Everbridge Limited and New World Telecommunications suppliers, both of this methods have a high level on the ranking, therefore they are good alternatives too.

Also, It is to highlight the low scores obtained by the cloud service provider Develloc us, it is the worst select of the providers list for MAUT and AHP methods, it has a great disadvantage compared to other providers. With Notorious Nine the results obtained are similar to those obtained previously for AHP and MAUT although the value of the weights of the criteria is different in this calculation.

In this final project has also carried out the analysis according to the type of provider (SaaS , IaaS and PaaS) , resulting in a high value for IaaS followed by SaaS and PaaS , as mentioned above is notable difference between the value obtained IaaS and PaaS.

Finally, all this in the case of selecting a provider of cloud services among the 12 analyzed, my choice would be iLand as in the case of MAUT is the provider that better data you get and also is a provider of IaaS(provides virtualized computing resources over the Internet) type which they have obtained an average score higher.

12.3 Future Work

This section describes possible future lines that could be made and that despite meeting the proposed objectives, a number of potential improvements and new implementations would add new features and enhancements include this application and the whole system will be explained. Possible ways to improve this work are as follows.

A possible future line would implement new multicriteria decision makers, an example would be the implementation of Swing Weights method. Once it has implemented new methods, we could compare the results obtained with other methods already in place.

Another future line would be the extension of the list of service providers Cloud to a much larger, As mentioned earlier , the version used in this Final Project is the latest , version 3.0.1, so that providers have used also belonged to this version. So an important upgrade is the expansion of the selection of suppliers to all including version 1.1. For this

improvement is needed in the implementation of the API the processing of all documents CAIQ v1.1, including all sub –groups.

Another improvement could be a new version of the design to a much more manageable by the client web application, for example with a new menu and with a new settings panel. These improvements would help create a much more professional application.

Finally , the addition of new charts showing the application of a more detailed way with the weights of each supplier for each criterion , or using more graphics iterative where the user can zoom the graph, it can also be a good improvement .

Parte VI

Planificación y Presupuesto

Capítulo 13
Planificación

13.1 Introducción

En este capítulo se van a realizar las distintas planificaciones llevadas a cabo para realizar este proyecto, a continuación se describen las distintas tareas con cada una de las fases realizadas.

13.2 Planificación inicial

En la planificación inicial se realiza una estructuración orientativa que se realizó al comienzo del proyecto:

- Reuniones y descripción del problema:

  Esta fase consiste en centrar la idea general y presentar las distintas iteraciones de cada tarea. En esta fase inicial del proyecto la reunión para describir el proyecto fue larga ya que se marcaban los pasos principales del proyecto.

  - Tiempo estimado: 6 horas.
  - Participantes: Desarrollador del Proyecto, tutor y Director.

- Documentación:

  En esta fase se llevó a cabo la documentación del proyecto, como fue la búsqueda de material sobre de los distintos métodos Multicriterio entre ellos constan AHP o MAUT:

  - Tiempo estimado: 25 horas.
  - Participantes: Desarrollador del Proyecto.

- Estudio:

  En esta fase se pretende que el desarrollador del proyecto se familiarice con los distintos métodos Multicriterio así como con el estudio de la planificación de la

aplicación web:

- Tiempo estimado: 30 horas.
- Participantes: Desarrollador del Proyecto.

- Implementación:

  En esta fase se incluye la planificación en el desarrollo completo de la aplicación:

  - Tiempo estimado: 160 horas.
  - Participantes: Desarrollador del Proyecto.

- Pruebas:

  En esta fase se realizan distintas pruebas para comprobar el funcionamiento correcto de la aplicación:

  - Tiempo estimado: 10 horas.
  - Participantes: Desarrollador del Proyecto.

- Presentación del proyecto:

  En esta fase se realiza la presentación de proyecto una vez entregada la memoria:

  - Tiempo estimado: 2 horas.
  - Participantes: Desarrollador del Proyecto.

13.3 Descomposición final en Tareas

En este apartado se realiza una estructuración final que se llevó a cabo en la realización de este proyecto:

Tarea 1: Despliegue y Funcionamiento servidor Web

- Subtarea 1.1: Instalación Apache Tomcat.
  - Descripción: En esta tarea se instala el servidor Web apache Tomcat.
  - Objetivos: Funcionamiento correcto para poder realizar las primeras pruebas.

- Relación otras tareas: Con esta tarea comienza el proyecto.
- Duración: 1 semana.
- Recursos: 0.1 Ingenieros / mes.

- Subtarea 1.2: Pruebas Servidor Apache Tomcat.
  - Descripción: En esta tarea se realizan pruebas para el servidor Web apache Tomcat.
  - Objetivos: Funcionamiento correcto para proseguir con el desarrollo de la aplicación.
  - Relación otras tareas: necesaria la subtarea 1.1.
  - Duración: 1 semana.
  - Recursos: 0.1 Ingenieros / mes.

Tarea 2: Documentación y análisis del Estado del Arte

- Subtarea 2.1: Estudio de los diferentes decisores Multicriterio.
  - Descripción: En esta tarea se estudian los diferentes decisores Multicriterio de manera general.
  - Objetivos: Conocimiento general de los distintos decisores.
  - Relación otras tareas: Con esta tarea comienza el desarrollo matemático del proyecto.
  - Duración: 2 semanas.
  - Recursos: 0.125 Ingenieros / mes.

- Subtarea 2.2: Estudio de los Procesos de Análisis Jerárquico.
  - Descripción: En esta tarea se estudia el proceso de análisis jerárquico para su futura implementación en el proyecto.
  - Objetivos: Conocimiento del proceso.

- Relación otras tareas: Necesaria la Tarea 2.1.
- Duración: 2 semana.
- Recursos: 0.125 Ingenieros / mes.

- Subtarea 2.3: Estudio de la Teoría de la Utilidad Multiatributo.
  - Descripción: En esta tarea se estudia el proceso de la Teoría de la Utilidad Multiatributo para su futura implementación en el proyecto.
  - Objetivos: Conocimiento del proceso.
  - Relación otras tareas: Necesaria la Tarea 2.1.
  - Duración: 2 semana.
  - Recursos: 0.125 Ingenieros / mes.

Tarea 3: Desarrollo Aplicación Web

- Subtarea 3.1: Diseño de la Aplicación Web.
  - Descripción: En esta tarea se realiza el diseño de la aplicación.
  - Objetivos: Creación de una aplicación.
  - Relación otras tareas: Con esta tarea comienza el desarrollo de la aplicación.
  - Duración: 1 semana.
  - Recursos: 0.525 Ingenieros / mes.

- Subtarea 3.2: Implementación de la Aplicación Web.
  - Descripción: En esta tarea se realiza el desarrollo de la aplicación.
  - Objetivos: Creación Aplicación.
  - Relación otras tareas: Necesario el punto 3.1.
  - Duración: 3 semanas.
  - Recursos: 0.525 Ingenieros / mes.

- Subtarea 3.3: Integración método AHP.
    - Descripción: En esta tarea se realiza la implementación del método AHP.
    - Objetivos: funcionamiento correcto del método.
    - Relación otras tareas: Necesario el punto 3.1 y 3.2.
    - Duración: 2 semanas.
    - Recursos: 0.525 Ingenieros / mes.
- Subtarea 3.4: Integración método MAUT.
    - Descripción: En esta tarea se realiza la implementación del método MAUT.
    - Objetivos: funcionamiento correcto del método.
    - Relación otras tareas: Necesario el punto 3.1 y 3.2.
    - Duración: 2 semanas.
    - Recursos: 0.525 Ingenieros / mes.
- Subtarea 3.5: Integración Notorious Nine.
    - Descripción: En esta tarea se realiza la implementación de Notorious Nine.
    - Objetivos: funcionamiento correcto del método.
    - Relación otras tareas: Necesario el punto 3.1 y 3.2.
    - Duración: 2 semanas.
    - Recursos: 0.525 Ingenieros / mes.
- Subtarea 3.6: Integración API.
    - Descripción: En esta tarea se realiza la integración con la API.
    - Objetivos: funcionamiento correcto.
    - Relación otras tareas: Necesario el punto 3.1, 3.2, 3.3.
    - Duración: 3 semanas.
    - Recursos: 0.525 Ingenieros / mes.

Tarea 4: Pruebas

- Subtarea 4.1: Pruebas de la Aplicación Web.
    - Descripción: En esta tarea se realizan las pruebas generales de la Aplicación Web.
    - Objetivos: Simulación de la aplicación.
    - Relación otras tareas: necesario todo lo anterior.
    - Duración: 1 semanas.
    - Recursos: 0.225 Ingenieros / mes.

- Subtarea 4.2: Pruebas de AHP en la Aplicación Web.
    - Descripción: En esta tarea se realizan las pruebas generales de la Aplicación Web para AHP.
    - Objetivos: Simulación de la aplicación.
    - Relación otras tareas: necesario todo lo anterior.
    - Duración: 1 semana.
    - Recursos: 0.225 Ingenieros / mes.

- Subtarea 4.3: Pruebas de MAUT en la Aplicación Web.
    - Descripción: En esta tarea se realizan las pruebas generales de la Aplicación Web para MAUT.
    - Objetivos: Simulación de la aplicación.
    - Relación otras tareas: necesario todo lo anterior.
    - Duración: 1 semana.
    - Recursos: 0.225 Ingenieros / mes.

- Subtarea 4.4: Pruebas Notorious Nine en la Aplicación Web.
    - Descripción: En esta tarea se realizan las pruebas generales de la Aplicación Web para Notorious Nine.
    - Objetivos: Simulación de la aplicación.

- Relación otras tareas: necesario todo lo anterior.
- Duración: 1 semana.
- Recursos: 0.225 Ingenieros / mes.

Tarea 5: Resultados

- Subtarea 5.1: Evaluación de los resultados.
  - Descripción: En esta tarea se estudian los resultados obtenidos.
  - Objetivos: Analizar los datos obtenidos y de las gráficas.
  - Relación otras tareas: necesario todo lo anterior.
  - Duración: 1 semana.
  - Recursos: 0.375 Ingenieros / mes.

Tarea 6: Memoria

- Subtarea 6.1: Organización y estructura de la memoria.
  - Descripción: Estudio de la memoria y su estructura.
  - Objetivos: Estructurar y organizar la memoria.
  - Relación otras tareas: comienza tras la tarea 5.
  - Duración: 1 semana.
  - Recursos: 0.125 Ingenieros / mes.

- Subtarea 6.2: Redacción de la memoria.
  - Descripción: Durante esta tarea se redacta el documento.
  - Objetivos: Redactar el contenido.
  - Relación otras tareas: comienza tras la tarea 6.1.

- Duración: 4 semanas.
- Recursos: 0.75 Ingenieros / mes.

- Subtarea 6.3: Redacción del resumen.
  - Descripción: Durante esta tarea se redacta el resumen de la memoria.
  - Objetivos: Redactar el resumen.
  - Relación otras tareas: comienza tras la tarea 6.2.
  - Duración: 1 semana.
  - Recursos: 0.125 Ingenieros / mes.

Tarea	Duración (semanas)	Recursos (Ing./m)
Despliegue y Funcionamiento servidor Web		
1.1: Instalación Apache Tomcat	1	0.1
1.2: Pruebas Servidor Apache Tomcat	1	0.1
Total		**0.2**
Documentación y análisis del Estado del Arte		
2.1: Estudio de los diferentes decisores Multicriterio.	2	0.125
2.2: Estudio de los Procesos de Análisis Jerárquico	2	0.125
2.3: Estudio de la Teoría de la Utilidad Multiatributo.	2	0.125
Total		**0.375**
Desarrollo Aplicación Web		
3.1: Diseño de la Aplicación Web.	1	0.525

3.2: Implementación de la Aplicación Web	3	0.525
3.3: Integración método AHP	2	0.525
3.4: Integración método MAUT	2	0.525
3.5: Integración Notorious Nine	2	0.525
3.6: Integración API	3	0.525
Total		**3.15**
Pruebas		
4.1: Pruebas de la Aplicación Web.	1	0.225
4.2: Pruebas de AHP en la Aplicación Web	1	0.225
4.3: Pruebas de MAUT en la Aplicación Web	1	0.225
4.4: Pruebas Notorious Nine en la Aplicación Web	1	0.225
Total		**0.9**
Resultados		
5.1: Evaluación de los resultados.	1	0.375
Total		**0.375**
Memoria		
6.1: Organización y Estructura de la memoria.	1	0.125
6.2: Redacción de la memoria	4	0.75
6.3: Redacción del Resumen	1	0.125
Total		**1**
Total		**6**

Figura 72. Tabla Planificación

13.4 Planificación con el diagrama de fases de ejecución detallado

La siguiente figura muestra la tabla de tareas principales y duración en días de cada una de ellas:

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
Tarea 1:Despliegue y Funcionamiento servidor Web	14 días	dom 01/02/15	sáb 14/02/15	
Tarea 2: Documentacion y analisis del Estado del Arte	42 días	sáb 14/02/15	vie 27/03/15	1
Tarea 3: Desarrollo de la Aplicación Web	91 días	vie 27/03/15	lun 22/06/15	2
Tarea 4:Pruebas	28 días	lun 22/06/15	dom 19/07/1	3
Tarea 5:Resultados	7 días	dom 19/07/15	dom 26/07/1	4
Tarea 6:Memoria	42 días	dom 26/07/15	sáb 05/09/15	5

Figura 73. Planificación Tareas Principales

La siguiente figura es un gráfico Gantt para las distintas tareas principales:

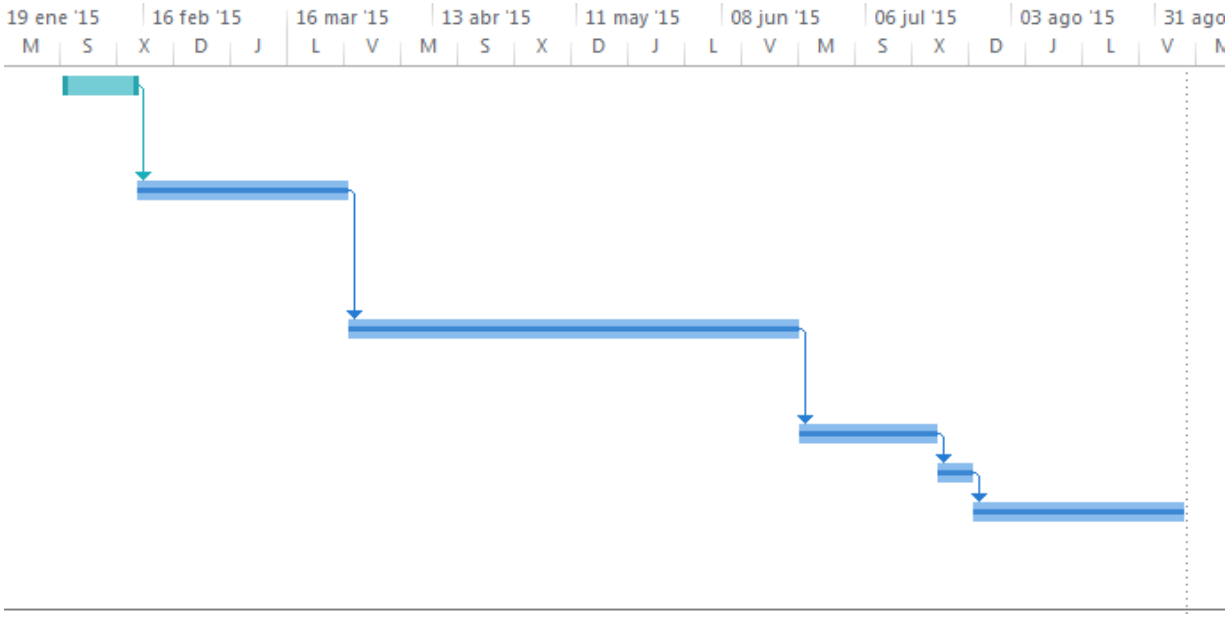


Figura 74. Gantt tareas principales

El gráfico de Gantt con todas las tareas que se han llevado a cabo en este Trabajo Fin de Grado es:

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
Tarea 1:Despliegue y Funcionamiento servidor Web	14 días	dom 01/02/15	sáb 14/02/15	
Instalacion Apache Tomcat	7 días	dom 01/02/15	sáb 07/02/15	
Pruebas Servidor	6 días	sáb 07/02/15	vie 13/02/15	2
Tarea 2: Documentacion y analisis del Estado del Arte	42 días	sáb 14/02/15	vie 27/03/15	1
Estudio decisores Multicriterio	14,5 días	vie 13/02/15	vie 27/02/15	3
Estudio AHP	14,5 días	vie 27/02/15	vie 13/03/15	5
Estudio MAUT	14 días	vie 13/03/15	vie 27/03/15	6
Tarea 3: Desarrollo de la Aplicación Web	91 días	vie 27/03/15	lun 22/06/15	4
Diseño	7 días	vie 27/03/15	jue 02/04/15	7
Implementación	21 días	jue 02/04/15	jue 23/04/15	9
Integración AHP	14 días	jue 23/04/15	mié 06/05/1	10
Integración MAUT	14 días	mié 06/05/15	mié 20/05/1	11
Integración Notorious Nine	14 días	mié 20/05/15	mar 02/06/15	12
Integración API	21 días	mar 02/06/15	lun 22/06/15	13
Tarea 4:Pruebas	28 días	lun 22/06/15	dom 19/07/1	8
Pruebas APP	7 días	lun 22/06/15	lun 29/06/15	14
Pruebas AHP	7 días	lun 29/06/15	lun 06/07/15	16
Pruebas MAUT	7 días	lun 06/07/15	lun 13/07/15	17
Pruebas Notorious Nine	7 días	lun 13/07/15	dom 19/07/15	18
Tarea 5:Resultados	7 días	dom 19/07/1	dom 26/07/1	15
Evaluacion de los resultados	7 días	dom 19/07/15	dom 26/07/15	19
Tarea 6:Memoria	42 días	dom 26/07/1	sáb 05/09/15	20
Organización y Estructura	7 días	dom 26/07/15	dom 02/08/15	21
Redaccion	28 días	dom 02/08/1	sáb 29/08/15	23
Resumen	7 días	sáb 29/08/15	sáb 05/09/15	24

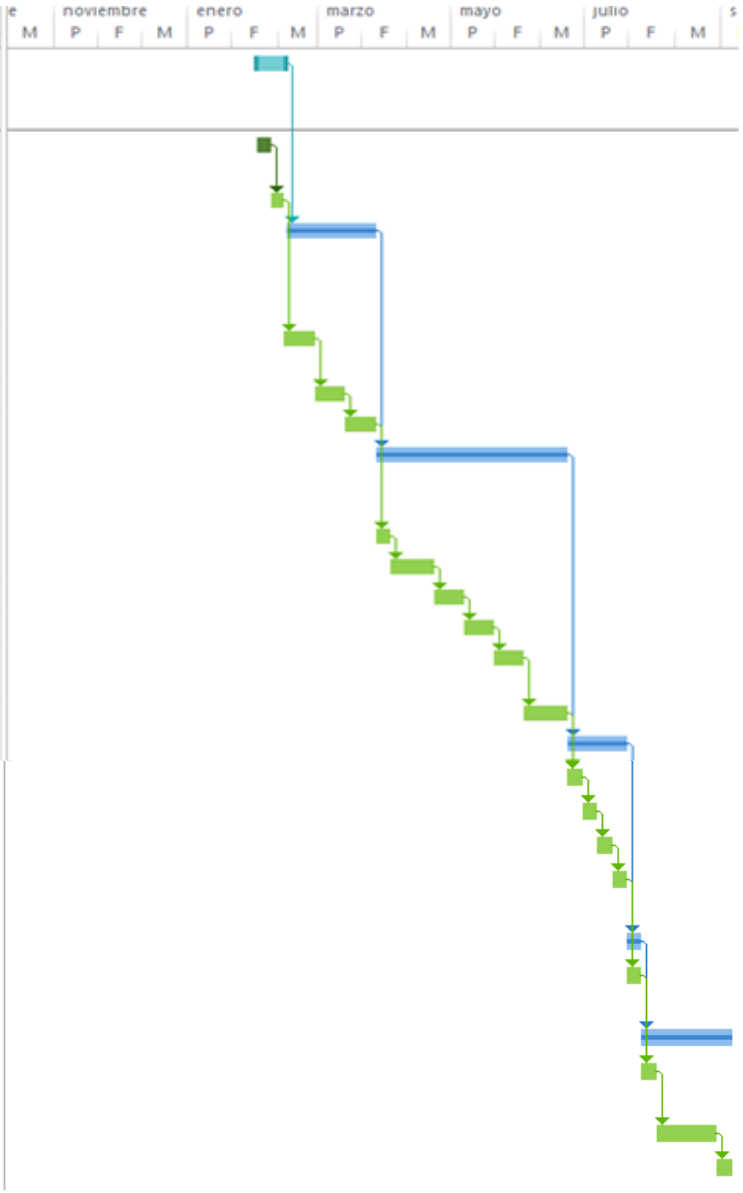


Figura 75.Gantt Tareas Detallado

Capítulo 14
Presupuesto

14.1 Recursos

En esta sección se describen los recursos necesarios para llevar a cabo el Trabajo Fin de Grado:

- Recursos Humanos:
    - 1 Graduado en Ingeniería en Tecnologías de la Telecomunicación: 6 ingenieros/mes.
    - 2 Ingenieros Senior: 0.5 ingenieros/mes.

- Recursos Materiales:
    - 1 Ordenador portátil HP Intel® Core™ i5-4210U con Sistema Operativo Linux.

      Este ordenador portátil ha sido utilizado para elaborar la mayoría del Trabajo Fin de Grado salvo la documentación y la redacción de la memoria.

        - Procesador Intel Core i5
        - Capacidad de Disco | 1 TB
        - Tarjeta gráfica nVIDIA GEFORCE 1 GB.

    - 1 Ordenador portátil ACER ASPIRE 5738PG con Sistema Operativo Windows.

      Este ordenador portátil ha sido usado para diferentes tareas como la documentación del proyecto, con la herramienta Microsoft Word.

        - Procesador Intel Core 2 Duo processor
        - Memoria RAM 4 GB.
        - Disco duro 500 GB HDD.

        - ATI Mobility Radeon HD 4570

- Otros recursos:
    - Conexión a Internet durante 8 meses.

14.2 Presupuesto del Proyecto

1. Autor: Iciar González González
1. Departamento: Ingeniería Telemática
2. Descripción del Proyecto:
    - Título: Selección de Proveedores de Servicios Cloud basado en métricas de seguridad.
    - Duración: 8 meses.
    - Tasa de costes indirectos: 20 %.
3. Presupuesto total del Proyecto (valorado en Euros): euros. Ver tabla 3
4. Subcontratación de tareas: no se especifican.
5. Otros costes directos del proyecto: no se especifican.

Concepto	Cantidad	Coste €	%Proyecto	Dedicación(meses)	Depreciación(meses)	Total €
Recursos Humanos						
▪ Graduado en Ingeniería de Tecnologías de telecomunicación.	1 (6 ing./mes)	2694.39	-	-	-	16166.34
▪ Ingenieros Senior	2 (0.5 ing./mes)	4289.54	-	-	-	2144.77
Total						**18311.11**
Recursos Materiales						
▪ Ordenadores portátiles	2	500	100	8	60	133.3
Total						**133.3**
Otros costes						
▪ Conexión a Internet	1	35	-	8	-	280
Total						**280**
Total						**18724.41 €**

Figura 76. Tabla Presupuesto

Parte VII

Anexos

Anexo A
Configuración Apache Tomcat

A.1 Introducción

En este apartado se va a describir la configuración necesaria para la instalación del Servidor Apache Tomcat.

A.2 Configuración

- Descargar Apache-Tomcat.

- Descomprimir el fichero deseado y copiar la carpeta en la ubicación deseada.

- Editar el fichero catalina.sh que se encuentra en la carpeta /opt/apache-tomcat-x.y.z/bin para añadir en el path la ruta donde tenemos la máquina virtual de java:

```
export PATH=${JAVA_HOME}/bin:${PATH}
```

- Compilar el fichero desde Apache:

```
javac -cp ${CATALINA_HOME}/lib/servlet-api.jar:. fichero.java
```

- Compilar los ficheros .java de la carpeta src:

```
javac -d ${CATALINA_HOME}/webapps/tfg/WEB-INF/classes -cp
${CATALINA_HOME}/webapps/tfg/WEB-
INF/classes:${CATALINA_HOME}/lib/servlet-api.jar *.java
proyecto/*.java
```

- En la misma carpeta bin, lanzamos Apache con:

```
./startup.sh.
```

Anexo B

Criterios utilizados para la decision de los Proveedores

B.1 Introducción

En este apartado se va a describir los criterios que se han utilizado para la decision a través de la metodología Multricriterio. La selección de criterios se agrupa según la granularidad deseada, si la granularidad es baja los criterios se organizaran según Control Group, si la granularidad es media será a través del CGID y si es alta a través de CID. A continuación se muestran las tablas de la organización propuesta por "CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1" [CON].

B.2 Criterios

Control Group	CGID	CID	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.
		AIS-01.2	
		AIS-01.3	
		AIS-01.4	
		AIS-01.5	
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, (removed all) identified security, contractual, and regulatory requirements for customer access shall be addressed.
		AIS- 02.2	
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alternation, or destruction.
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures and compliance obligations.
		AAC-02.2	
		AAC-02.3	
		AAC-02.4	
		AAC-02.5	
		AAC-02.6	
		AAC-02.7	

		AAC-02.8	
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1 AAC-03.2 AAC-03.3 AAC-03.4	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1 BCR-01.2	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1 BCR-03.2	Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications,and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1 BCR-07.2 BCR-07.3 BCR-07.4 BCR-07.5	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment
Business Continuity Management &	BCR-09	BCR-09.1 BCR-09.2	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must

Operational Resilience *Impact Analysis*		BCR-09.3	incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1 BCR-11.2 BCR-11.4 BCR-11.5	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1 CCC-01.2	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1 CCC-02.2	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1 CCC-03.2 CCC-03.3 CCC-03.4	Organization shall follow a defined qualty change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, as well as infrastructure network and systems components. Technical measures shall be implemented to provide assurance that, prior to deployment, all changes directly correspond to a registered change request, business-critical or customer (tenant) , and/or authorization by, the customer (tenant) as per agreement (SLA).
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1 DSI-01.2 DSI-01.3 DSI-01.4 DSI-01.5 DSI-01.6 DSI-01.7	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1 DSI-02.2	Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.
Data Security &	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks

Information Lifecycle Management *eCommerce Transactions*		DSI-03.2	shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1 DSI-04.2	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1 DSI-07.2	Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.
Datacenter Security *Asset Management*	DCS-01	DCS-01.1 DCS-01.2	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership y defined roles and responsibilities.
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.
Datacenter Security *Offsite equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.
Datacenter Security *Policy*	DCS-06	DCS-06.1 DCS-06.2	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1 EKM-02.2 EKM-02.3 EKM-02.4 EKM-02.5	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.
Encryption & Key	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes

Management *Encryption*		EKM-03.2 EKM-03.3 EKM-03.4	and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1 EKM-04.2 EKM-04.3 EKM-04.4	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1 GRM-01.2 GRM-01.3	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1 GRM-02.2	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance
		GRM-04.2	
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.
Governance and Risk Management *Policy*	GRM-06	GRM-06.1 GRM-06.2 GRM-06.3 GRM-06.4	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1 GRM-07.2	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.

Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1 GRM-09.2	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1 GRM-10.2	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).
Governance and Risk Management *Program*	GRM-11	GRM-11.1 GRM-11.2	Organizations shall develop and maintain an enterprise risk management framework to mitigate risk to an acceptable level.
Human Resources *Asset Returns*	HRS-01	HRS-01.1 HRS-01.2	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.
Human Resources *Employment Agreements*	HRS-03	HRS-03.1 HRS-03.2 HRS-03.3 HRS-03.4 HRS-03.5	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.
Human Resources *Employment Termination*	HRS-04	HRS-04.1 HRS-04.2	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.
Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).
Human Resources *Nondisclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.
Human Resources *Acceptable Use*	HRS-08	HRS-08.1 HRS-08.2 HRS-08.3	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.
Human Resources *Training / Awareness*	HRS-09	HRS-09.1 HRS-09.2	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.
Human Resources *User Responsibility*	HRS-10	HRS-10.1 HRS-10.2 HRS-10.3	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment
Human Resources	HRS-11	HRS-11.1 HRS-11.2	Policies and procedures shall be established to require that unattended

Workspace		HRS-11.3	workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1 IAM-01.2	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1 IAM-02.2	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1 IAM-04.2	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.
Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1 IAM-06.2	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1 IAM-07.2 IAM-07.3 IAM-07.4 IAM-07.5 IAM-07.6 IAM-07.7	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1 IAM-08.2	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.
Identity & Access	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants),

Management *User Access Authorization*		IAM-09.2	business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1 IAM-10.2 IAM-10.3	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1 IAM-11.2	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1 IAM-12.2 IAM-12.3 IAM-12.4 IAM-12.5 IAM-12.6 IAM-12.7 IAM-12.8 IAM-12.9 IAM-12.10 IAM-12.11	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1 IAM-13.2 IAM-13.3	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1 IVS-01.2 IVS-01.3 IVS-01.4 IVS-01.5	Higher levels of assurance are required for protection, retention, and lifecyle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1 IVS-02.2	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1 IVS-04.2 IVS-04.3 IVS-04.4	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1 IVS-06.2 IVS-06.3 IVS-06.4	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.

Infrastructure & Virtualization Security *OS Hardening and Base Conrols*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.
Infrastructure & Virtualization Security *Production / Nonproduction Environments*	IVS-08	IVS-08.1 IVS-08.2 IVS-08.3	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1 IVS-09.2 IVS-09.3 IVS-09.4	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection*	IVS-10	IVS-10.1 IVS-10.2	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1 IVS-12.2 IVS-12.3	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1 IVS-13.2	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.
Interoperability & Portability *APIs*	IPY-01	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.
Interoperability & Portability *Data Request*	IPY-02	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1 IPY-03.2	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage and integrity persistence.
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1 IPY-04.2	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1 IPY-05.2	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.

Mobile Security *Anti-Malware*	MOS-01	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.
Mobile Security *Application Stores*	MOS-02	MOS-02	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.
Mobile Security *Approved Applications*	MOS-03	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.
Mobile Security *Awareness and Training*	MOS-05	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.
Mobile Security *Cloud Based Services*	MOS-06	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.
Mobile Security *Compatibility*	MOS-07	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.
Mobile Security *Device Eligibility*	MOS-08	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.
Mobile Security *Device Inventory*	MOS-09	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD), will be included for each device in the inventory.
Mobile Security *Device Management*	MOS-10	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.
Mobile Security *Encryption*	MOS-11	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1 MOS-12.2	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and isenforced through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).
Mobile Security *Legal*	MOS-13	MOS-13.1 MOS-13.2	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required.
Mobile Security *Lockout Screen*	MOS-14	MOS-14	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.
Mobile Security *Operating Systems*	MOS-15	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.
Mobile Security *Passwords*	MOS-16	MOS-16.1 MOS-16.2 MOS-16.3	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.
Mobile Security *Policy*	MOS-17	MOS-17.1 MOS-17.2 MOS-17.3	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1 MOS-18.2	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.
Mobile Security *Security Patches*	MOS-19	MOS-19.1 MOS-19.2	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.
Mobile Security *Users*	MOS-20	MOS-20.1 MOS-20.2	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.

Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1 SEF-02.2 SEF-02.3 SEF-02.4	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1 SEF-03.2	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1 SEF-04.2 SEF-04.3 SEF-04.4	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1 SEF-05.2	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01	STA-01.1 STA-01.2	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1 STA-03.2	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.
Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05	STA-05.1 STA-05.2 STA-05.3 STA-05.4	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business

		STA-05.5	relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07	STA-07.1 STA-07.2 STA-07.3 STA-07.4	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.
		STA-8.2	
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09	STA-09.1 STA-09.2	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.
Threat and Vulnerbility Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1 TVM-01.2	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
Threat and Vulnerbility Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1 TVM-02.2 TVM-02.3 TVM-02.4 TVM-02.5 TVM-02.6	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.
Threat and Vulnerbility Management *Mobile Code*	TVM-03	TVM-03.1 TVM-03.2	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

Glosario

La lista de los acrónimos utilizados en este Trabajo Fin de Grado son:

AHP: *Analytic Hierarchy Process*

API: *Application Programming Interface*, conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

ASF: *Apache Software Foundation,* organización no lucrativa creada para dar soporte a los proyectos de software bajo la denominación Apache, incluyendo el popular servidor HTTP Apache.

CAGT: *Compounded Annual Growth Rate,* término específico de negocios e inversión para la ganancia anualizada lisa de una inversión sobre un periodo dado de tiempo.

CAI: *Consensus Assessment Initiative*, iniciativa orientada a proporcionar transparencia en los servicios Cloud mediante la documentación de los controles de seguridad de dichos servicios.

CSA: *Cloud Security Alliance*, organización sin ánimo de lucro dedicada a promover la investigación sobre las mejores prácticas para ofrecer garantías de seguridad en Cloud Computing.

CSP: *Cloud Service Provider*, proveedor de servicios Cloud.

HTML: *HyperText Markup Language,* lenguaje de marcado para la elaboración de páginas web. Es un estándar que, en sus diferentes versiones, define una estructura básica y un código para la definición de contenido de una página web, como texto, imágenes, etc.

HTTP: *Hypertext Transfer Protocol,* protocolo usado en cada transacción de la World Wide Web.

IaaS: *Infrastructure As A Service,* en español Infraestructura como Servicio. Modelo de distribución de infraestructura de computación como un servicio, normalmente mediante una plataforma de virtualización

IT: *Information Technology, t*ecnología necesaria para adquirir, almacenar, procesar y distribuir información por medios electrónicos: radio, televisión, teléfono,

computadoras.

JSON: *JavaScript Object Notation*, es un formato ligero para el intercambio de datos. JSON es un subconjunto de la notación literal de objetos de JavaScript que no requiere el uso de XML.

JSP: *JavaServer Pages*, tecnología que ayuda a los desarrolladores de software a crear páginas web dinámicas basadas en HTML, XML, entre otros tipos de documentos.

MAUT: *Multi-Attribute Utility Theory.*

MCDA: *Multiple-Criteria Decision Analysis.*

MCDM: *Multiple-Criteria Decision-Making.*

MUI: *Mutuamente Independientes en Utilidad*, las preferencias por las apuestas sobre un atributo son independientes de la cantidad del otro atributo.

PaaS: *Platform As A Service,* en español Plataforma como Servicio. Aunque suele identificarse como una evolución de SaaS, es más bien un modelo en el que se ofrece todo lo necesario para soportar el ciclo de vida completo de construcción y puesta en marcha de aplicaciones y servicios web.

PNG: *Portable Network Graphics*, es un formato gráfico basado en un algoritmo de compresión sin pérdida para bitmaps no sujeto a patentes.

SaaS: *Software As A Service,* en español Software como Servicio. Modelo de distribución de software donde una empresa sirve el mantenimiento, soporte y operación que usará el cliente durante el tiempo que haya contratado el servicio.

STAR: *Registro de Seguridad, Confianza y Garantías*, mecanismo de certificación de proveedores Cloud a través de un registro público que contiene los controles de seguridad proporcionados por los proveedores (CCM y CAIQ).

XML: *eXtensible Markup Language*, es un lenguaje de marcas desarrollado por el World Wide Web Consortium (W3C) utilizado para almacenar datos en forma legible.

Referencias

[TRI+98] E. Triantaphyllou, B. Shu, S. Nieto Sanchez, and T. Ray. *Multi-Criteria Decision Making: An Operations Research Approach*. Louisiana State University, 1998.

[ZIM91] Zimmermann, H.-J., Fuzzy Set Theory and Its Applications, Kluwer Academic Publishers, Second Edition, Boston, MA, 1991.

[TOS+05] Toskano Hurtado, Gérard Bruno. *El Proceso de Análisis Jerárquico (AHP) como Herramienta para la Toma de Decisiones en la Selección de Proveedores para la Empresa Gráfica Comercial MyE S.R.L*. Lima 2005.

[OSO+08] Osorio Gómez, Juan Carlos; Orejuela Cabrera, Juan Pablo. *El proceso de análisis jerárquico (AHP) y la toma de decisiones Multicriterio. Ejemplo de Aplicación.* Universidad Tecnológica de Pereira 2008

[HO+06] Ho, W., Dey, P. K. y Higson, H. (2006): *Multiple criteria decision-making techniques in higher education, International Journal of Educational Management*, vol. 20, no. 5, pp. 319-337.

[FRA+11] Francisco Llamazares Redondo, Sergio A.Berumen. *Los métodos de decisión Multicriterio y su aplicación al análisis del desarrollo local*. 2011

[CSA] Cloud Security Alliance. *The Notorious Nine Cloud Computing Top Threats in 2013.*Febrero 2013.

[KEE+76] Keeney, R.L. y Raiffa, H., 1976. *Decisions with multiple objectives: Preferences and value tradeoffs*. New York: John Wiley and Sons.

[KEE96] Keeney, R.L., 1996. *Value-focused thinking: a path to creative decision making*. Harvard University Press. USA.

[HWA+81] Hwang, C.L. y K. Yoon., 1981. *Multiple attribute decision making*. Springer-Verlag. Berlin.

[ARA+97] Aragonés B.P. y Gómez-Senent M.E., 1997. *Técnicas de Ayuda a la Decisión Multicriterio.* Cuaderno de Apuntes. Departamento de la Construcción y de Proyectos de Ingeniería Civil. Editorial de la Universidad Politécnica de Valencia. Valencia.

[SEP03] Seppälä, J. 2003. *Life cycle impact assessment based on decision analysis.* Tesis Doctoral. Helsinki University of Technology. Department of Engineering Physics and Mathematics. System Analysis Laboratory. Research Report A86, June 2003. Espoo, Findland.

[YOO+95] Yoon, K.P. y Hwang, C.L., 1995. *Multiple attribute decision-making: An introduction. Sage University paper series on quantitative applications in the social sciences*, 07-104. Thousands Oaks, CA. Sage

[SAA80] T.L. Saaty*. The Analytic Hierarchy Process, Planning, Piority Setting, Resource Allocation*. McGraw-Hill, New York, 1980

[SAA+98] T.L. Saaty and L.G. Vargas*. Diagnosis with dependent symptoms: Bayes theorem and the analytic hierarchy process.* Operations Research, 46(4):491-502, 1998.

[MAS+08] Masud, Abu S. M.; Ravindran, A. Ravi. *Multiple criteria decision making.*2008

[SAA96] Saaty, T.L. *Decision Making With Dependence And Feedback: The Analytic Network Process*. Pittsburgh: RWS Publications.1996.

[VAL12] *La decisión Multicriterio; aplicación en la selección de ofertas competitivas en edificación*. Master en Edificación. Universidad Politécnica de Valencia. 2012.

[RAM01] Sánchez, Ramiro. *La toma de decisiones con múltiples criterios. Un resumen conceptual y teórico.* Centro de Planificación y Gestión, Universidad Mayor de San Simón. 2001

[SAA94] SAATY, T.L. *Fundamentals of Decision Making.* RSW Publications.1994

[EDU01] Eduardo Miranda. *Improving subjective estimates using paired comparisons.* IEEE Software, 18(1):87-91, Jan/Feb 2001.

[ZOP+02] C.Zopounidis y M.Doumpos. *Multi–criteria Classification Methods in Financial and Banking Decisions.* 16 DEC 2002

[HER+99] Herwijnen, M. van and P.Rietveld .*Spatial Dimensions in Multicriteria Analysis. 1999*

[APA] APACHE SOFTWARE FOUNDATION. http://www.apache.org/free/. Último acceso Septiembre 2015.

[GOO] GOOGLE DEVELOPERS. https://developers.google.com/chart/interactive/docs/security_privacy. Último acceso Septiembre 2015.

[CON] https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/ . Último acceso Septiembre 2015.

[IDC] https://www.idc.com/getdoc.jsp?containerId=prUS25576415 Último acceso Septiembre 2015.

[SER07] Alonso Blázquez, F., Serrano Bárcena, N. y Calzada Mínguez, S. Informática II. Capítulo 9: Servlets. Universidad de Navarra, 2007

Cloud services provider selection based on security metrics

One of the technological services that is in full development and use by many industries is Cloud Computing. Over time we have witnessed the many changes that have hit the technology sector but few advances have been as significant as the development of this service as well as the entry of numerous global providers that offer it. Cloud services allow a large number of companies to gain ubiquitous and on demand access to a shared set of computing resources, which has supposed a revolution that benefits both the end consumer and the public or private companies. The security in this service has been one of the main problems, as the user data happen to be stored in outside servers, for all this, the safety aspects are of key importance as outsourcing infrastructure (IaaS), platform (PaaS) and (SaaS) software to a third party which handles our data.

There are organizations such as Cloud Security Alliance (CSA), which promotes the use of best practices for securing cloud computing and provides security education and guidance to companies. These practices include the assessment of the risk of contracting a cloud service provider (CSP) or the analysis of the security requirements based on company needs. CSA provides a useful tool for selecting cloud service providers called Consensus Cloud Assessment Initiative (CAI), a questionnaire that allows assessing the security management of a provider according to answers. However, this process can be tedious and complex for customers.

Moreover, at the present time, the exploration of greater productivity and efficiency encourage the search for new methods to cope with decision-making in settings where many selection criteria or alternatives are involved. For all these reasons, it is necessary to use tools to discern between alternatives for obtaining, to the greatest extent possible, the most satisfactory solution as well as the provider that most security grant us is of primary importance. In this search of new methodologies we find the multicriteria decision methods in which this project focuses.

If we combine the increased demand for cloud services and the number of providers that offer this service with multicriteria decision methods, we obtain as a result the search for maximum efficiency through proper selection of a provider that best suits the criteria selected by the client. Within these criteria, security aspects have a fundamental importance to select the right provider according to the level of protection that they need.

Thus, the idea of this project arises: to create a tool that automatically make that cloud service assessment easily for the customer. This tool would be composed of two parts:

- An engine that manages and analyses data security metrics of cloud services providers and a Web service to access that data.

- A web application that allows comparing with Multicriteria methods and graphically the security services from different CSPs using the data provided by the Web service.

The final tool is integrated by two related projects that implement each of the parts as is shown in Figure 1.

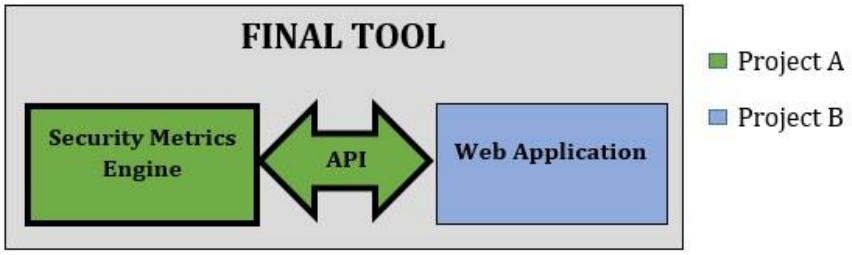


Figure 77. Tool structure

In particular, this project corresponds to the Project B shown in Figure 1. The goal of this project is, through the collection of metadata, perform the best provider selection based in security metrics with the use of multi-criteria methods. In this Final Project we study two types of methodologies based on multi-criteria decision making mechanisms to discern between different cloud service providers, these methodologies are: first, Analytic Hierarchy Process (AHP) and, secondly, Multiattribute Utility Theory (MAUT).

Multi-Criteria Decision Making has developed a common terminology [MAS+08] which includes concepts such as:

- Attributes: are the characteristics, features, parameters or qualities that describe each of the alternatives. The number of chosen attributes will be decided by the decision maker or group choice.

- Alternatives: are the possible solutions to the problem of decision that the decision maker can choose.

- Criteria: are the parameters that allow reflecting the preferences of the decision maker regarding an attribute.

- Objectives: indicate the directions of improvements as provided by the decision maker. It is a statement of something you want to achieve [KEE96].

- Goals: the alternative that will collect already established attributes and can meet the criteria selected as close as possible to the stated objectives.

The first method developed in this Final Project is the Analytic Hierarchy Process (AHP) which is a structured technique for dealing with complex decisions, it was developed in the late 60s by Thomas L.Saaty who from his research in the military field along with his experience made this tool. With its simplicity it has been implemented in thousands of applications through which important results have been obtained. AHP is a structured methodology to measure and synthesize well as a mathematical method created to evaluate alternatives when we take into consideration several criteria.

The main feature of the AHP is modeled by a hierarchy [Figure 2] whose apex is the main objective or goal to achieve ,at intermediate levels ,criteria are displayed and selected on the basis of which the decision is made finally, at base, are the alternatives to be evaluated. This design hierarchy requires experience and a good understanding of the problem as it requires all the necessary information. The second defining characteristic of this method is that each level of hierarchy is based on the use of comparisons between pairs of elements from these comparisons are constructed whereby matrix, and using matrix algebra, priorities are established with respect to an element of the next higher level. These pairwise comparisons are performed using ratios of importance or preference, and these weights or priorities should add one unit. In short, the AHP method is a decision model that interprets data using trials and measured on a scale of reason within a hierarchical structure.

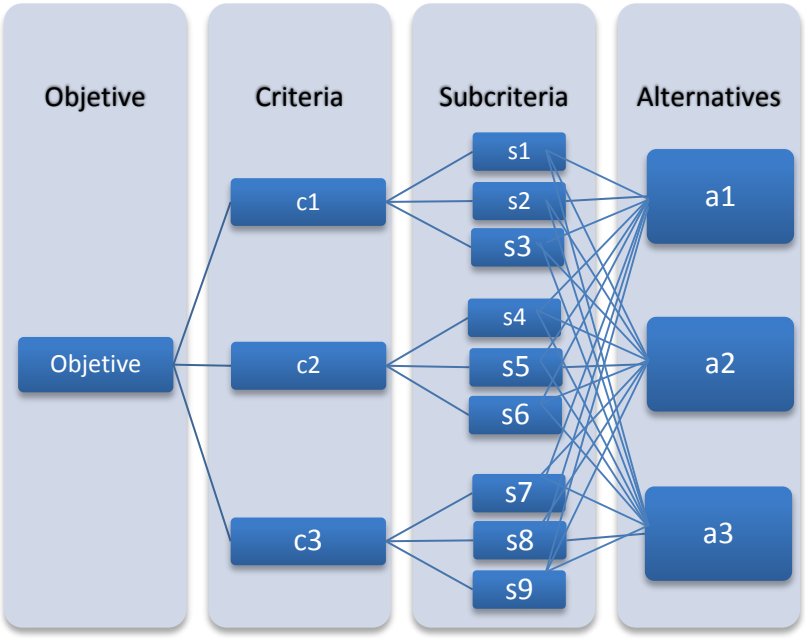


Figure 2 .Hierarchical model for decision with AHP

As a first step, an appropriate selection criteria is an essential stage in the decision-making process, once you have defined the criteria and sub-criteria forming a descending hierarchy [Figure 2] should be made to build the entire hierarchy where in the last level the alternatives are placed, the next step is to build a weight vector that evaluates the relative importance attached to each criterion. The AHP method uses an indirect assignment in which the decision maker made an assessment in qualitative terms and, once on the scale, the numerical values corresponding to that value is obtained. The scale of values suggested by Saaty [SAA80] is shown in Figure 3:

Intensity of importance	Definition
1	Equal importance
2	Weak
3	Moderate importance
4	Moderate plus
5	Strong importance
6	Strong plus
7	Very strong or demonstrated importance
8	Very, very strong
9	Extreme importance

Figure 3. Scale of relative importance (according to Saaty (1977; 1980)).

The other method studied is Multiattribute Utility Theory (Multi-Attribute Utility Theory - MAUT), is one of the most popular multicriteria decision making methodologies, provides a strong axiomatic basis for rational decision-making under multiple objectives [SEP03] used functions utility to convert numerical scales in useful attributes that allow a direct comparison of various measures, ie express the preferences of the decision maker in terms of the utility that reports (principle of rationality).

The main phases for the correct application of MAUT are:

1. Structuring a hierarchy of attributes: the decision-maker makes a set of attributes for the problem.

2. Definition of the utility functions: for each attribute a utility function that translates as an evaluator whose anger utility value between 0 and 1 is defined.

3. Transformation of preferences weights: weights are used to characterize the importance of different attributes. These weights can be obtained by various methods.

4. Characterization of the alternatives: for each alternative attributes need to be evaluated qualitatively or quantitatively.

5. Aggregation of results: For each alternative attributes are transformed into a utility function from step 2 and weighted with weights from step 3.

AHP differs from MAUT on how to get the judgments of the decision maker and the basic principles to set preferences for this. The MAUT objective is to find a simple expression for the net benefits of a decision by the utility functions. It is based on the assumption that the decision maker is rational, having a perfect and consistent in their judgments knowledge, the aim of the decision maker will be to maximize the utility value as low values in some criteria can be compensated by high scores other. For all this, MAUT is a type of MCDA known as "compensatory methods". For AHP, this method added various facets to the problem of decision with a single function optimization, it aims to select the alternative with greater weight and MCDA is a type known as "compensatory optimization."

On the design carried out in the application, the Criteria selection, following Consensus Assessment Initiative (CAI), which is oriented to provide transparency in Cloud services by documenting security controls initiative, this results in the creation of a document called CAIQ (CAI Questionnaire) which is an Excel document containing a questionnaire, in tabular form, about the different security controls that meet a particular Cloud service. There are two versions of the document: version 1.1 and version 3.0.1. In this Final Project will use version 3.0.1. The following image shows a fragment of the document CAIQ which has different categories, the first one is the category Control Group (CG) that contains the different groups that include controls with common characteristics. These groups fall into domains, represented in the document with different colors. The domains are defined by the different critical security areas in Cloud Computing. The next column corresponds to each group identifiers (CGID). The document describing the characteristics of the group is also included. Here are the basic controls, submitted by an identifier (CID). In this application the user can select a category or the other depending on the granularity you choose, in the case of low CG are selected, in the case of half the CGID and in the case of high CID.

Control Group	CGID	CID	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1 AIS-01.2 AIS-01.3 AIS-01.4 AIS-01.5	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.

Figure 4. Fragment of the document CAIQ.

For the selection of the providers, the data is obtained through the Registry Security, Trust and Guarantees (STAR) which is a mechanism of certification of cloud providers through a public register containing security controls developed by the organization CSA. This record includes a list of providers or CSP (Cloud Service Provider) whose documents are published for the evaluation of its cloud services. The selected providers, as first selection criterion is that the type of document provided by the company to be CAI Questionnaire and other criteria is the version found in the CAIQ documents may be in the initial release version 1.1 and more 3.0.1 recent since you'll use is the 3.0.1 providers who will use that version will be also. The providers include in this application are:

Provider
Adallom
Capriza
Caretower
DataNoah
Develloocus
Everbridge
HKT
ILand
New World Telecommunications Ltd
OneLogin
Perfecto Mobile
Zscaler

Figure 5. Providers List.

The development of the web application that comprises the system of selecting cloud service providers based on security metrics was made progressively following a dynamic methodology as possible. We find integration with external server metadata, it is a API REST (Representational State Transfer) which is a type of architecture development that relies entirely on the standard HTTP and allows us to create services and applications that can be used by any device or client who understands HTTP. Those providers metadata are obtained from the API. The end result of application design is shown in Figure 6:

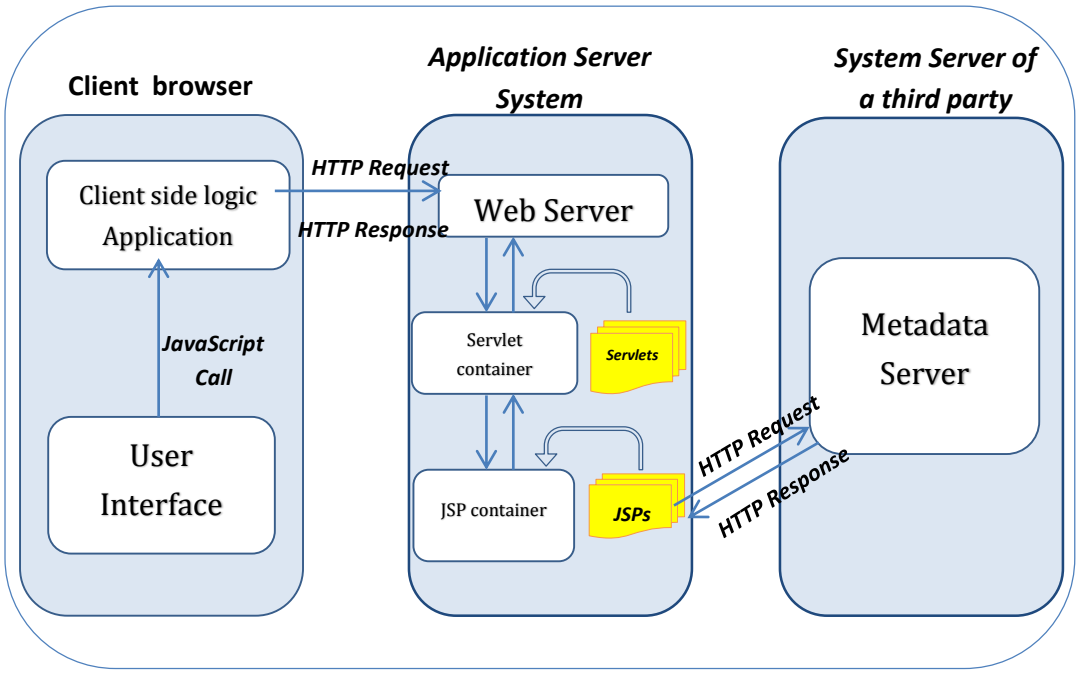


Figure 6. Application design

For the results, we tested with 12 providers, with public safety metadata based on 16 criteria belonging to a low granularity. With this configuration test, we evaluate the different providers and the main conclusion in the case of analysis by the methods of Multi-criteria decision in the case of Hierarchical Analysis Process (AHP) and the Multi-attribute Utility Theory (MAUT) highlights the high value obtained for Cloud service providers Perfect Mobile and iLand for different criteria, we must also highlight the low value obtained for both methods for Develocus provider, being more remarkable the difference in value compared to other providers using MAUT. We must also emphasize the high value obtained for both of methodologies Everbridge or New World Telecommunications Limited. They are also a good choice.

In this Final Project also it develops from the list of the Notorious Nine [CSA] the decision Multricriterio through the methods seen, for they shall be weighted according to the criteria appearing on the list. The purpose of the report: "The Notorious Nine: Cloud Computing Top Threats in 2013" [CSA] is to provide organizations with an updated view of the threats to the security of the cloud in order to conduct risk management properly and a right relationship strategies to manage the cloud. The results obtained are similar to those obtained previously for AHP and MAUT although the value of the weights of the criteria is different in this calculation.

It has also been analyzed according to the different forms it can take the cloud. The providers used in this analysis can be divided into:

- Infrastructure as a Service (IaaS): In this case the processing capacity (CPU) and storage contracts.

- Software as a Service (SaaS): In this case it is an application for the end user where rent for the use of the software is paid. .

- Platform as a Service (PaaS): there is further provided an application server and a database.

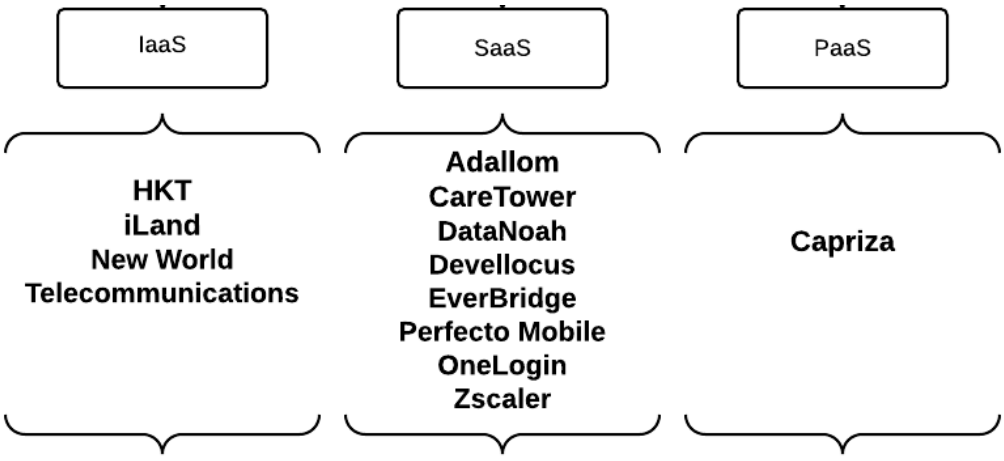


Figure 7. Providers Cloud Type

To numerically analyze the data, we have calculated the mean of the weights obtained for each type of provider. With these data we can conclude that the type of cloud that greater value obtained is the IaaS with a very high average score, followed by SaaS and finally PaaS group which was only formed by Capriza, we should mention the average value as distant between the type of Cloud IaaS and PaaS type, which becomes 36% to MAUT.

Finally, all this in the case of selecting a provider of cloud services among the 12 analyzed, my choice would be iLand as in the case of MAUT is the provider that better data you get and also is a provider of IaaS(provides virtualized computing resources over the Internet) type which they have obtained an average score higher.

References

[CSA] Cloud Security Alliance. *The Notorious Nine Cloud Computing Top Threats in 2013.*Febrero 2013.

[KEE96] Keeney, R.L., 1996*. Value-focused thinking: a path to creative decision making*. Harvard University Press. USA.

[MAS+08] Masud, Abu S. M.; Ravindran, A. Ravi. *Multiple criteria decision making.*2008

[SAA80] T.L. Saaty*. The Analytic Hierarchy Process, Planning, Piority Setting, Resource Allocation*. McGraw-Hill, New York, 1980

[SEP03] Seppälä, J. 2003. *Life cycle impact assessment based on decision analysis.* Tesis Doctoral. Helsinki University of Technology. Department of Engineering Physics and Mathematics. System Analysis Laboratory. Research Report A86, June 2003. Espoo, Findland.